Úvod do teorie množin

Poznámky k předmětu NAIL063

Jakub Smolík

smolikj@matfyz.cz

Datum poslední změny:
5. července 2026

Úvodní slovo

Tento text slouží jako skriptíčka k předmětu NAIL063, vyučovaného na MFF UK. Je založen na mých poznámkách z roku 2024, kdy tento předmět vyučoval docent Jan Kynčl. Přednáška vychází z první a začátku druhé kapitoly učebnice Balcara a Štěpánka [1]. Velmi hezké povídání o základech teorie množin, které napsal Mirek Olšák, je také na webu matematického korespondenčního semináře [5].

Pokud jste v textu našli nějaký překlep nebo chybu, ať už stylistickou, či matematickou, napište mi prosím na `smolikj@matfyz.cz`.

Obsah

1 Cantorova naivní teorie množin

Naivní teorií myslíme teorii, která nemá formálně dané axiomy. Místo toho se na její popis používá přirozený jazyk. Na množiny pohlíží jako na soubory libovolných „věcí“. Tento přístup je intuitivní a ve většině případů zcela dostačující. Běžně v matematice pracujeme s množinami tímto způsobem a ničemu to nevadí. Ale ukáže se, že to vede k celé řadě paradoxů.

Sám Cantor si byl například vědom toho, že jeho teorie připouští existenci množiny všech množin, přestože z Cantorovy věty vyplývá, že množina všech množin neexistuje. Tento paradox ale nebyl natolik zásadní, aby donutil Cantora přehodnotit svoji teorii.

Pravděpodobně ten nejdůležitější paradox, který nadobro pohřbil Cantorovu naivní teorii a dal vzniknout axiomatickým teoriím množin, byl Russelův paradox.

1.1 Russelův paradox

Jako první ho zřejmě objevil matematik Ernst Zermelo roku 1899, ale své zjištění nezveřejnil. Publikoval ho až Russell v roce 1901. Návrh první teorie, která se tomuto paradoxu snažila vyhnout, přišel od Zermela v roce 1908. Matematik Abraham Fraenkel ovšem roku 1921 poukázal na to, že v Zermelově teorii není možné dokázat existenci některých množin, jejichž existenci většina tehdejších množinových teoretiků považovala za samozřejmou. Následující rok navrhl úpravu axiomů této teorie, čímž vznikla dnes velmi rozšířená Zermelo–Fraenkelova teorie množin (ZF).

Definice 1.1. Množina M je *krotká* pokud $M \notin M$; jinak je *divoká.*

Například *množina všech zvířat* je krotká, zatímco *množina všech věcí, které nejsou čajové lžičky* je divoká. Zajímavá je třeba *množina všech věcí, na které právě myslím.* Většinou je krotká, ale právě teď, když píšu tuto větu, je divoká.

Podívejme se na množinu všech krotkých množin $M := \{x \mid x \textit{ je krotká}\}$. Je krotká, nebo divoká? Pokud je krotká, potom splňuje definiční podmínku M, tedy $M \in M$, takže je divoká. Pokud je divoká, potom nesplňuje definiční podmínku M, tedy $M \notin M$, takže je krotká. Čili je krotká $\iff$ je divoká.

Russelův paradox nám ukazuje, že musíme nějak omezit, co vše může být množinou.

1.2 Berryho paradox

Berryho paradox naopak ukazuje, že definice pomocí přirozeného jazyka mohou vést k paradoxům. Proto se budeme snažit věci definovat jazykem matematické logiky. Paradox zní následovně:

Označme m nejmenší přirozené číslo, které nelze definovat méně než sto písmeny.

Anglická abeceda + mezera = 27 znaků, takže celkem 27^{100} kombinací, tedy takovéto m existuje. Víme, že m nelze definovat méně než sto znaky, ale věta výše (která má určitě méně než sto znaků) jej definuje.

2 Nejprve trochu logiky

2.1 Jazyk teorie množin

Jazyk teorie množin je $\langle \in \rangle$ s rovností, kde $\in$ je binární relační symbol. Mohli bychom uvažovat i jazyk bez rovnosti a přidat nový binární relační symbol '$=$' a axiomy rovnosti. V každém jazyku je implicitně

- spočetně mnoho symbolů pro proměnné: $x_1, x_2, x_3, \dots,$
- pro každou proměnnou x dva symboly s kvantifikátory: $(\forall x)$, $(\exists x)$,
- symboly pro logické spojky a pro negaci: $\neg$, $\wedge$, $\vee$, $\implies$, $\iff$,
- čárka a závorky.

Tento jazyk ještě rozšíříme o několik zkratek. Konkrétně definujme

- $x \neq y \equiv \neg x = y$,
- $x \notin y \equiv \neg x \in y$,
- $x \subseteq y \equiv (\forall z)(z \in x \Rightarrow z \in y)$,
- $x \subset y \equiv x \subseteq y \wedge x \neq y$,
- $x \in y \in z \equiv x \in y \wedge y \in z$,

kde '$\equiv$' vyjadřuje, že výraz nalevo bude od teď ekvivalentní výrazu napravo.

2.2 Termy a formule

Nyní uvažujme obecný jazyk L s množinou relačních symbolů $\mathcal{R}$ a množinou funkčních symbolů $\mathcal{F}$. Konstantní symboly jsou funkční symboly arity nula.

Definice 2.1. *Termy* jazyka L jsou konečné nápisy definované induktivně:

- každá proměnná a každý konstantní symbol z L je term,
- pro funkční symbol f arity n a termy $t_1, \dots, t_n$ je term i nápis $f(t_1, \dots, t_n)$.

Definice 2.2. *Atomická formule* je nápis $R(t_1, \dots, t_n)$, kde R je n-ární relační symbol a t_i jsou termy.

Definice 2.3. *Formule* jazyka L jsou konečné nápisy definované induktivně:

- každá atomická formule jazyka L je formule,
- jsou-li φ a ψ formule, potom jsou formule i nápisy

$$(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi), (\varphi \Leftrightarrow \psi), ((\forall x)\varphi), ((\exists x)\varphi).$$

Formule mají přirozenou stromovou strukturu. *Výskyt* proměnné x je list tohoto stromu označený x. *Podformule* jsou podstromy tohoto stromu.

Definice 2.4 (Volné a vázané proměnné)**.** Výskyt proměnné x ve formuli φ je

- *vázaný*, pokud se vyskytuje v nějaké podformuli začínající $(\forall x)$ nebo $(\exists x)$,
- *volný*, pokud není vázaný.

Proměnná x je

- *vázaná* ve formuli φ, pokud má vázaný výskyt ve φ.
- *volná* ve formuli φ, pokud má volný výskyt ve φ.

Úmluva 2.5. Zápis $\varphi(x_1, \ldots, x_n)$ značí, že $x_1, \ldots, x_n$ jsou proměnné, jejichž volné výskyty nás ve formuli φ zajímají. Neznamená to, že každá z proměnných x_i musí mít volný výskyt ve φ, ani že φ neobsahuje žádné jiné volné proměnné.

Příklad. Uvažme formuli $\varphi = (\forall x)(\exists y)(x \leq y) \vee (x \leq z)$. Kvantifikátory se vztahují pouze k první závorce $(x \leq y)$. Proměnná x je vázaná a volná zároveň, y je vázaná a z je volná. Můžeme tedy psát $\varphi(x, z)$.

3 Axiomy Zermelo–Fraenkelovy teorie množin

Až doposud mohly množiny obsahovat libovolné „věci“ a vlastně jsme nijak nespecifikovali, co přesně jsou tyto věci zač. V axiomatické teorii množin existují pouze ty objekty, jejichž existence vyplývá z axiomů dané teorie. Axiomy ZF nám garantují existenci prázdné množiny a poskytují nám několik způsobů jak z již existujících množin vyrábět nové. Jinými slovy: všechno je množina. Každý prvek každé množiny je jen nějaká jiná množina.

3.1 Axiom existence

Axiom 3.1. Existuje nějaká množina, univerzum množin není prázdné.

$$(\exists x)(x = x).$$

3.2 Axiom extenzionality

Axiom 3.2. Množina není dána ničím jiným než svými prvky.

$$(\forall z)(z \in x \Leftrightarrow z \in y) \implies x = y.$$

Je důležité zdůraznit, že toto *není* definice identity dvou množin. Musíme vnímat odděleně dva koncepty. První koncept je naše teorie, ve které můžeme dokazovat různá pravdivá tvrzení. Je to něco zcela abstraktního. Druhý koncept je nějaká konkrétní „implementace“ (model) této teorie. Symbol ‘=’ hovoří o identitě objektů, které poskytne ta konkrétní implementace. My „zevnitř“ naší teorie vůbec netušíme, jak by tato implementace mohla vypadat. Ale máme „zvenčí“ poskytnutý symbol =, který smíme používat. Každá implementace „ví“, co tento symbol znamená. Ale neví, co znamená symbol $\in$. Axiomy jsou nějaké požadavky, které musí každý model splňovat. Takže tento axiom není definice identity dvou množin, protože identita je koncept, který je odtržený od teorie a přísluší až konkrétnímu modelu. Tento axiom vyjadřuje vztah symbolu $\in$ a identity a každý model bude muset tento požadavek splnit. Opačná implikace,

$$x = y \implies (\forall z)(z \in x \Leftrightarrow z \in y),$$

platí také, ale není součástí axiomu extenzionality, protože vlastně říká, že

$$(\forall z)(z \in x \Leftrightarrow z \in x),$$

což platí pro libovolnou implementaci symbolu $\in$.

3.3 Axiom dvojice

Axiom 3.3. Pro každou dvojici množin x a y existuje množina d, která obsahuje právě x a y. Množinu d značíme jako $\{x, y\}$.

$$(\forall x, y)(\exists d)(\forall z)\big(z \in d \Leftrightarrow (z = x \vee z = y)\big).$$

Tento axiom zaručuje i existenci jednoprvkových množin $\{x\} := \{x, x\}$.

3.4 Axiom sumy

Axiom 3.4. Pro každou množinu x existuje množina s, která je sjednocením všech množin uvnitř x. Této množině říkáme *suma* množiny x a značíme ji $\bigcup x$.

$$(\forall x)(\exists s)(\forall z)\big(z \in s \Leftrightarrow (\exists y)(y \in x \wedge z \in y)\big).$$

Pozorování 3.5. *Pokud $x \in y \in z$, potom $x \in \bigcup z$.*

Nyní můžeme pomocí kombinace axiomu sumy a axiomu dvojice definovat sjednocení dvou množin a libovolně velkou konečnou množinu danou výčtem.

Definice 3.6. *Sjednocení* množin x a y je množina $x \cup y := \bigcup\{x, y\}$.

Definice 3.7. Množiny $\{x_1\}$ a $\{x_1, x_2\}$ jsou garantované axiomem dvojice. Množinu $\{x_1, x_2, \ldots, x_n\}$ definujeme induktivně jako $\{x_1, x_2, \ldots, x_{n-1}\} \cup \{x_n\}$.

Příklad. $\bigcup\big\{\{x_1\}, \{x_1, x_2\}, \{x_2, x_3\}\big\} = \{x_1, x_2, x_3\}$.

3.5 Schéma axiomů vydělení

Schéma znamená, že se nejedná o jeden konkrétní axiom, ale o nekonečně mnoho různých axiomů, které mají všechny stejnou strukturu.

Axiom 3.8. Pokud je x množina, potom existuje množina všech jejích prvků, které splňují formuli φ. Tuto množinu značíme $\{z \in x \mid \varphi(z)\}$. Formálně, je-li $\varphi(z)$ formule, která neobsahuje volně proměnnou y, potom formule

$$(\forall x)(\exists y)(\forall z)\big(z \in y \Leftrightarrow (z \in x \wedge \varphi(z))\big).$$

je axiom.

Všimněme si, že schéma axiomů vydělení nám nedovoluje vyrobit množinu všech množin nebo množinu všech krotkých množin, protože neumožňuje konstrukce typu $\{z \mid \varphi(z)\}$. Použitím axiomu vždy vznikne podmnožina nějaké již existující množiny. Například z množiny X, garantované axiomem existence, lze vyrobit prázdnou množinu tak, že za φ zvolíme libovolnou nesplnitelnou formuli.

Definice 3.9. *Prázdná množina* je množina $\emptyset := \{z \in X \mid z \neq z\}$.

Také konečně můžeme nadefinovat průnik a rozdíl množin.

Definice 3.10. *Rozdíl* množin x a y je množina $x \setminus y := \{z \in x \mid z \notin y\}$.

Definice 3.11. *Průnik* množin x a y je množina $x \cap y := \{z \in x \mid z \in y\}$.

Definice 3.12. Množiny x a y jsou *disjunktní* pokud $x \cap y = \emptyset$.

Definice 3.13. *Průnik* množiny $x \neq \emptyset$ je množina $\bigcap x := \big\{z \in \bigcup x \mid y \in x \Rightarrow z \in y\big\}$.

Příklad. Průnik konečně mnoha množin $x_1, x_2, \ldots, x_n$ lze zapsat dvěma způsoby:

$$\bigcap\{x_1, x_2, \ldots, x_n\} = x_1 \cap x_2 \cap \cdots \cap x_n.$$

Průnik nekonečně mnoha množin už ovšem lze udělat pouze jako průnik nekonečné množiny x.

Poznámka. Důvod, proč zatím nedefinujeme průnik prázdné množiny je ten, že s touto definicí bychom měli $\bigcap\varnothing = \varnothing$, což moc nedává smysl. Prázdný součet je nula, prázdný součin je jedna a prázdná suma je prázdná množina. Vše to jsou neutrální prvky vůči dané operaci. Co je neutrální prvek vůči průniku? Prázdná množina určitě ne. Nabízí se množina všech množin, ale ukážeme, že ta neexistuje. Tento problém vyřešíme v sekci 4.2.

Definice 3.14. *Uspořádaná dvojice* (a, b) je množina $\{\{a\}, \{a, b\}\}$. Uspořádanou n-tici $(a_1, a_2, \ldots, a_n)$ potom definujeme induktivně jako $((a_1, a_2, \ldots, a_{n-1}), a_n)$.

Lemma 3.15. *Uspořádaná dvojice určuje své prvky jednoznačně. Tedy*

$$(x, y) = (a, b) \iff (x = a \wedge y = b).$$

Důkaz. Nejprve '$\Leftarrow$'. Z axiomu extenzionality máme $\{x\} = \{a\}$ a $\{x, y\} = \{a, b\}$ a tedy i $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$. Nyní '$\Rightarrow$'. Ukážeme, že (a,b) jednoznačně určuje pořadí svých prvků. Označme $P \coloneqq \bigcap(a,b)$ a $S \coloneqq \bigcup(a,b)$. Potom platí

$$\{a\} = P, \quad \{b\} = \{z \in S \mid z \neq a \vee P = S\}. \qquad \square$$

3.6 Axiom potence

Axiom 3.16. Pro každou množinu x existuje množina všech jejích podmnožin. Této množině říkáme *potenční množina* množiny x a značíme ji $\mathcal{P}(x)$.

$$(\forall x)(\exists p)(\forall z)(z \in p \Leftrightarrow z \subseteq x).$$

Pozorování 3.17. *Potenční množina a suma jsou svým způsobem opačné operace:*

$$z \subseteq x \Rightarrow z \in \mathcal{P}(x), \qquad z \in x \Rightarrow z \subseteq \bigcup x, \qquad \bigcup \mathcal{P}(x) = x \subseteq \mathcal{P}\big(\bigcup x\big)$$

3.7 Schéma axiomů nahrazení

Axiom 3.18. Když si vezmeme libovolné zobrazení F a množinu vzorů A, tak množina obrazů $B = F[A]$ je také množina. Formálně, je-li $\psi(x, y)$ formule, která neobsahuje volně proměnné y_1, y_2 a b, potom formule

$$(\forall x)(\forall y_1,y_2)\big((\psi(x, y_1) \wedge \psi(x, y_2)) \Rightarrow y_1 = y_2\big) \Rightarrow \\ (\forall a)(\exists b) : (\forall y)\big(y \in b \Leftrightarrow (\exists x)(x \in a \wedge \psi(x, y))\big)$$

je axiom. Formule $\psi(x, y_1)$, respektive $\psi(x,y_2)$ vznikne z formule $\psi(x, y)$ substitucí proměnné y_1, respektive y_2 za y.

První část tohoto axiomu říká, že $\psi(x,y)$ se má chovat jako zobrazení $y = F(x)$. Ve druhé polovině značí a množinu vzorů a b množinu obrazů, které těmto vzorům odpovídají.

Pozorování 3.19. *Pokud za $\psi(x,y)$ zvolíme formuli $x = y \wedge \varphi(y)$, tak je první část axiomu nahrazení splněna. Tedy platí, že*

$$(\forall a)(\exists b)(\forall y)\big(y \in b \Leftrightarrow (\exists x)(x \in a \wedge x = y \wedge \varphi(y))\big),$$

což je jen trochu jinak zapsaný axiom vydělení.

3.8 Axiom fundovanosti

Axiom 3.20. Každá neprázdná množina obsahuje nějakou množinu, která je s ní disjunktní.

$$(\forall a \neq \varnothing)(\exists x \in a)(x \cap a = \varnothing).$$

Tedy pro všechny množiny $y \in a$ máme $y \notin x$; jinými slovy, x je $\in$-minimální prvek množiny a.

Důsledek 3.21. *Neexistuje množina a splňující $a \in a$.*

Důkaz. Pro spor nechť a je divoká. Potom množina $\{a\}$ nesplňuje fundovanost, protože $a \in a$ a zároveň $a \in \{a\}$, takže $a \in a \cap \{a\}$. □

Důsledek 3.22. *Neexistuje dvojice množin a, b taková, že $a \in b$ a $b \in a$. Tentokrát poruší fundovanost množina $\{a, b\}$.*

Tento axiom nám zaručuje, že v ZF nemůže vzniknout Russelův paradox, protože vylučuje možnost existence divokých a dalších divných množin. Také z něj vyplývá, že v ZF neexistuje množina všech množin, protože ta by určitě byla divoká. Mohlo by se zdát, že axiom fundovanosti je hodně důležitý, ale není: existence divokých množin nám nevadí, protože ostatní axiomy nám neumožňují vytvořit množinu všech divokých množin (byla by to takzvaná *vlastní třída*). A to, že množina všech množin neexistuje, se dá dokázat i bez axiomu fundovanosti.

To neznamená, že axiom fundovanosti nemá žádný význam — umožňuje některé elegantní konstrukce a argumenty, ale my se s nimi nesetkáme.

3.9 Axiom nekonečna

Axiom 3.23. Existuje nekonečná množina s nějakou konkrétní strukturou.

$$(\exists w)\big(\varnothing \in w \wedge (\forall z)(z \in w \Rightarrow z \cup \{z\} \in w)\big).$$

Axiom nekonečna nám umožní definovat množinu všech přirozených čísel jako nejmenší (vzhledem k inkluzi) množinu splňující tuto podmínku.

3.10 Axiom výběru a ZFC

Axiom výběru, anglicky Axiom of Choice (AC), je natolik silné tvrzení, že není součástí základní verze Zermelo–Fraenkelovy teorie množin. Jeho přidáním do ZF získáme teorii ZFC. Je důležité zmínit, že přestože ZFC je výrazně silnější než ZF, tak Gödel v roce 1940 ukázal, že pokud je ZF konzistentní,[1] potom je ZFC také konzistentní. Čili to, zda věříme nebo nevěříme axiomu výběru, je čistě filozofické rozhodnutí, na konzistenci teorie množin to nic nezmění.

Bez axiomu výběru nelze dokázat mnoho věcí, které by intuitivně měly platit, ale některé jeho důsledky jsou na hranici paradoxnosti, proto byl historicky poměrně kontroverzní. Budeme se jím zabývat ve zvláštní kapitole, ale intuitivně říká, že pokud nám někdo dá libovolnou množinu A, potom z každé neprázdné množiny $X \in A$ lze *vybrat* nějaký konkrétní prvek $x \in X$, a posléze všechny tyto prvky posbírat a vytvořit novou množinu, která je všechny obsahuje.

[1] Tedy má model, nebo ekvivalentně, není v ní možné dokázat spor.

4 Množiny a třídy

Abychom zabránili Russelovu paradoxu, museli jsme omezit, co vše je množinou. Ale občas se hodí mluvit o souboru všech objektů, které něco splňují, přestože to už není množina. Proto se zavádí pojem *třída.* V Cantorově naivní teorii jsou třídy a množiny jedno a totéž. Pokud omezíme, co všechno může být množinou, tak se náš svět rozdělí:

- Množiny — někam náleží.
- Třídy — něco náleží do nich.

Uvědomme si, že tento koncept neumožňuje zrekonstruovat Russellův paradox, jelikož třída všech krotkých tříd zjevně neexistuje. Třídy totiž nemohou nikam náležet, věci pouze náleží do nich.

4.1 Rozšíření jazyka o třídové termy

Předpokládejme, že pracujeme v nějakém konkrétním modelu M teorie množin s univerzem množin $\mathbf{V}$.

Definice 4.1 (Třídový term)**.** Pokud $\varphi(z, v_1, \ldots, v_n)$ je formule a $y_1, \ldots, y_n$ jsou množiny z $\mathbf{V}$, potom výraz $\{z \,|\, \varphi(z, y_1, \ldots, y_n)\}$ nazýváme *třídový term.*

Třídy jsou pouze mata-jazykový pojem sloužící k zjednodušení zápisu. Nejsou to formální objekty ZF. Pokud pro množinu x z $\mathbf{V}$ napíšeme

$$x \in \{z \,|\, \varphi(z, y_1, \ldots, y_n)\},$$

tak tím myslíme, že $\varphi(x, y_1, \ldots, y_n)$ platí.[2] Třídové termy tedy definují nějaké „soubory“ množin, které splňují příslušnou formuli, a tyto soubory nazýváme *třídy.*

Každou množinu lze interpretovat jako třídu, a některé třídy lze interpretovat jako množiny, ale ne všechny.

Pozorování 4.2. *Každá množina je zároveň i třídou, protože $x = \{z \,|\, z \in x\}$.*

Pozorování 4.3. *Pokud $\varphi(z)$ je ve tvaru $z \in y \wedge \psi(z)$, kde y je množina, pak třída $\{z \,|\, \varphi(z)\}$ je množinou (z axiomu vydělení).*

Definice 4.4. Třídu, která není množinou, nazýváme *vlastní třída.*

Například ukážeme, že třída všech množin,

$$\mathbf{V} = \{x \,|\, x = x\},$$

také nazývanou *univerzální třída*, je vlastní třídou.

Ve formulích na místě volných proměnných připustíme třídové termy. Navíc dovolíme třídové proměnné, které budeme značit velkými písmeny. Ale pouze jako volné proměnné, takže třídy není možné kvantifikovat.

Definice 4.5 (Formule s třídovými termy)**.** Atomické formule v tomto rozšířeném jazyce jsou

$$x = y, \quad x \in y, \quad x = X, \quad x \in X, \quad X \in x, \quad X = Y, \quad X \in Y,$$

kde x, y jsou proměnné, X je zkratka za $\{z \,|\, \varphi(z)\}$ a Y za $\{z \,|\, \psi(z)\}$.

Každá atomická formule je formule a libovolná kombinace formulí pomocí logických spojek je opět formule. Množinové proměnné lze navíc kvantifikovat.

[2] Přesněji řečeno, instance formule φ, která vznikne substitucí množin $y_1, \ldots, y_n$ za volné proměnné $v_1, \ldots, v_n$, platí v modelu M.

Tvrzení 4.6. *Pro každou formuli s třídovými termy, ale bez třídových proměnných, existuje ekvivalentní formule v základním jazyce.*

Důkaz. Všechny atomické formule s třídovými termy přepíšeme do základního jazyka. Mějme množinu x a třídové termy $X = \{z \,|\, \varphi(z)\}$ a $Y = \{y \,|\, \psi(y)\}$, kde formule φ a ψ neobsahují volně proměnné u a v.

- $x \in X \sim x \in \{z \,|\, \varphi(z)\} \sim \varphi(x)$,
- $X = Y \sim \{z \,|\, \varphi(z)\} = \{z \,|\, \psi(z)\} \sim (\forall u)(\varphi(u) \Leftrightarrow \psi(u))$.

Dále budeme využívat, že X nemůže být vlastní třída.

- $x = X \sim x = \{z \,|\, \varphi(z)\} \sim (\forall u)(u \in x \Leftrightarrow \varphi(u))$,
- $X \in Y \sim \{z \,|\, \varphi(z)\} \in \{z \,|\, \psi(z)\} \sim (\exists u)\big(u = \{z \,|\, \varphi(z)\} \wedge u \in \{z \,|\, \psi(z)\}\big) \sim (\exists u)\big((\forall v)(v \in u \Leftrightarrow \varphi(v)) \wedge \psi(u)\big)$,
- $X \in x \sim \{z \,|\, \varphi(z)\} \in x \sim (\exists u)\big(u = \{z \,|\, \varphi(z)\} \wedge u \in x\big) \sim (\exists u)\big((\forall v)(v \in u \Leftrightarrow \varphi(v)) \wedge u \in x\big)$. □

Důsledek 4.7. *Formule rozšířeného jazyka určují stejné třídy jako formule základního jazyka. Z toho také vyplývá, že již definované třídy můžeme používat pro definování tříd nových.*

Přestože třídové proměnné nelze kvantifikovat, neznamená to, že nemůžeme dokázat nějaké tvrzení typu „pro každou třídu X platí něco strašně zajímavého co už nekvantifikuje přes žádné další třídové proměnné“ Formálně říkáme, že pro každou třídu X platí nějaká formule $\psi(X)$ bez třídových proměnných (využívá pouze třídový term X), která je podle předchozího tvrzení ekvivalentní nějaké formuli $\bar{\psi}(X)$ základního jazyka. Tohle říct můžeme, pouze to nebude jediná věta, ale *schéma* vět: pro každou formuli $\varphi(z, v_1, \ldots, v_n)$ budeme mít jednu větu ve tvaru

$$(\forall y_1)(\forall y_2) \cdots (\forall y_n)\, \bar{\psi}\big(\{z \,|\, \varphi(z, y_1, \ldots, y_n)\}\big).$$

Podobné schéma lze udělat pro každé tvrzení, které má libovolný (konečný) počet univerzálních třídových kvantifikátorů, ale žádné existenční třídové kvantifikátory. Těch už se podobným trikem nezbavíme, leda, že by důkaz byl konstruktivní. Pokud například tvrdíme, že pro každou třídu existuje nějaká jiná třída, tak ji musíme explicitně zkonstruovat.

Úloha 4.8. Zapište formálně, pomocí základního jazyka teorie množin, tvrzení, že všechny třídy, s výjimkou prázdné množiny, obsahují alespoň jeden prvek.

Definice 4.9. Rozšíříme náš jazyk o další zkratky. Nechť A je třída a φ formule.

- $(\exists x \in A)(\varphi) \equiv (\exists x)(x \in A \wedge \varphi)$,
- $(\nexists x \in A)(\varphi) \equiv (\forall x)(x \notin A \vee \neg\varphi)$,
- $(\forall x \in A)(\varphi) \equiv (\forall x)(x \in A \Rightarrow \varphi)$.

Poslední zkratku definujeme pouze pro formule $\varphi(x)$ bez volných výskytů y a z:

- $(\exists! x \in A)(\varphi) \equiv (\exists x \in A)(\varphi) \wedge (\forall y \in A)(\forall z \in A)\big((\varphi(y) \wedge \varphi(z)) \Rightarrow y = z\big)$.

4.2 Třídové operace

Definice 4.10. Pro třídy A a B definujeme

- $A \cap B \coloneqq \{x \mid x \in A \wedge x \in B\}$,
- $A \cup B \coloneqq \{x \mid x \in A \vee x \in B\}$,
- $A \setminus B \coloneqq \{x \mid x \in A \wedge x \notin B\}$, ... případně $A - B$
- $\bigcup A \coloneqq \{x \mid (\exists a)(a \in A \wedge x \in a)\}$,
- $\bigcap A \coloneqq \{x \mid (\forall a)(a \in A \Rightarrow x \in a)\}$
- $A \subseteq B \iff (\forall x)(x \in A \Rightarrow x \in B)$, ... A je *podtřídou* B
- $A \subset B \iff A \subseteq B \wedge A \neq B$, ... A je *vlastní podtřídou* B
- $\mathcal{P}(A) \coloneqq \{x \mid x \subseteq A\}$.

Pozorování 4.11. *Průnik prázdné množiny $\bigcap \varnothing$ je třída všech množin $\mathbf{V}$.*

Úloha 4.12. Ukažte, že $\mathcal{P}(\mathbf{V}) = \mathbf{V}$.

Lemma 4.13. *Je-li x množina a $X = \{z \mid \varphi(z)\}$ třída, potom je $x \cap X$ množina.*

Důkaz. Z axiomu vydělení, protože $x \cap X = \{z \in x \mid \varphi(z)\}$. □

4.3 Kartézský součin

Definice 4.14. *Kartézský součin* tříd X a Y je třída

$$X \times Y \coloneqq \{(x, y) \mid x \in X \wedge y \in Y\}.$$

Kartézský součin tříd $X_1, X_2, \ldots, X_n$ definujeme induktivně jako

$$X_1 \times \cdots \times X_n \coloneqq (X_1 \times \cdots \times X_{n-1}) \times X_n = \{(x_1, \ldots, x_n) \mid \textstyle\bigwedge_{i=1}^{n} x_i \in X_i\}.$$

Lemma 4.15. *Jsou-li x a y množiny, potom je $x \times y$ také množina.*

Důkaz. Idea těchto důkazů: najít nějakou hodně velkou množinu a pak použít axiom vydělení. Dokážeme, že platí

$$x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y)).$$

Uspořádanou dvojici jsme definovali jako $(a, b) = \{\{a\}, \{a, b\}\}$. Pokud $a \in x$ a $b \in y$, tak $\{a\}, \{a, b\} \subseteq x \cup y$ neboli $\{a\}, \{a, b\} \in \mathcal{P}(x \cup y)$. Tedy $(a, b) \subseteq \mathcal{P}(x \cup y)$, z čehož $(a, b) \in \mathcal{P}(\mathcal{P}(x \cup y))$. □

Definice 4.16 (Kartézská mocnina)**.** Pro třídu X definujeme $X^1 \coloneqq X$ a pak induktivně $X^n \coloneqq X^{n-1} \times X$.

Pozorování 4.17. *Pro univerzální třídu platí $\mathbf{V} = \mathbf{V}^1 \supseteq \mathbf{V}^2 \supseteq \mathbf{V}^3 \supseteq \cdots$.*

Důkaz. Každá n-tice je i dvojice (tak je definována), ale lze ji dokonce vnímat jako k-tici pro libovolné $k \leq n$. Například jako trojici $(a, b, c) = ((a, b), c)$:

$$(x_1, \ldots, x_{n-1}, x_n) = ((x_1, \ldots, x_{n-1}), x_n) = (((x_1, \ldots, x_{n-2}), x_{n-1}), x_n).$$ □

Příklad. Definujeme $X^3 \coloneqq X^2 \times X$, ale $X \times X^2 \neq X^3$. Mají stejnou strukturu, ale v teorii množin to jsou různé objekty. Zvolme třeba $X = \{\varnothing\}$. Máme

- $X^2 \times X = \{(\varnothing, \varnothing)\} \times \{\varnothing\} = \{((\varnothing, \varnothing), \varnothing)\}$,
- $X \times X^2 = \{\varnothing\} \times \{(\varnothing, \varnothing)\} = \{(\varnothing, (\varnothing, \varnothing))\}$.

4.4 Relace a zobrazení

Definice 4.18. *Binární relace* je libovolná třída $R \subseteq \mathbf{V} \times \mathbf{V}$. Namísto $(x,y) \in R$ píšeme $x\,R\,y$. Podobně lze definovat *n-ární relaci* jako $R \subseteq \mathbf{V}^n$.

Definice 4.19. Pro (binární) relaci R a třídu X definujeme třídy

- $R^{-1} \coloneqq \{(v,u) \mid u\,R\,v\}$, … *inverzní relace* k relaci R
- $\mathrm{Dom}(R) \coloneqq \{u \mid (\exists v)(u\,R\,v)\}$, … *definiční obor* relace R
- $\mathrm{Rng}(R) \coloneqq \{v \mid (\exists u)(u\,R\,v)\}$, … *obor hodnot* relace R
- $R \restriction X \coloneqq R \cap (X \times \mathbf{V}) \subseteq R$, … *zúžení relace* R na třídu X
- $R[X] \coloneqq \mathrm{Rng}(R \restriction X) \subseteq \mathrm{Rng}(R)$. … *obraz* třídy X relací R

Pozorování 4.20. $R \subseteq \mathrm{Dom}(R) \times \mathrm{Rng}(R), \quad R^{-1} \subseteq \mathrm{Rng}(R) \times \mathrm{Dom}(R)$.

Lemma 4.21. *Pokud je relace x množina a Y třída, potom x^{-1}, $\mathrm{Dom}(x)$, $\mathrm{Rng}(x)$, ale i $x \restriction Y$ a $x[Y]$ jsou také množiny.*

Důkaz. Pomocí axiomu vydělení.

- Ukážeme $\mathrm{Dom}(x) \subseteq \bigcup(\bigcup x)$. Pro každé $u \in \mathrm{Dom}(x)$ platí $(u,v) \in x$ pro nějaké v. Máme posloupnost inkluzí $u \in \{u\} \in (u,v) \in x$, tedy $u \in \bigcup(\bigcup x)$.
- Podobně $\mathrm{Rng}(x) \subseteq \bigcup(\bigcup x)$, zkrátka to $v \in \mathrm{Rng}(x)$ je třeba vybalit z té uspořádané dvojice $(u,v) \in x$ jako $v \in \{u,v\} \in (u,v) \in x$.
- $x^{-1} \subseteq \mathrm{Rng}(x) \times \mathrm{Dom}(x)$ protože kartézský součin množin je množina.
- $x[Y] \subseteq \mathrm{Rng}(x)$ a $x \restriction Y \subseteq x$. □

Definice 4.22. Relace odpovídající relačním symbolům jazyka teorie množin jsou

- $\mathbf{E} \coloneqq \{(x,y) \mid x \in y\}$, … *náležení*
- $\mathbf{Id} \coloneqq \{(x,y) \mid x = y\}$. … *identita*
- $\Delta_X \coloneqq \mathbf{Id} \restriction X$ … *identita na třídě X*

Definice 4.23 (Skládání relací)**.** Pro relace R a S definujeme relaci

$$R \circ S \coloneqq \{(u,w) \mid (\exists v)(u\,R\,v \wedge v\,S\,w)\}$$

Příklad. $\mathbf{Id} \circ R = R \circ \mathbf{Id} = R, \quad (x,y) \in \mathrm{E} \circ \mathrm{E} \iff x \in \bigcup y$.

Definice 4.24 (Zobrazení)**.** Relace F je *zobrazení* (nebo *funkce*) pokud

$$(\forall u)(\forall v)(\forall w)\big(((u,v) \in F \wedge (u,w) \in F) \Rightarrow v = w\big).$$

Namísto $u\,F\,v$ píšeme $F(u) = v$, při definování píšeme $F : u \mapsto v$ nebo $F(u) \coloneqq v$.

Pozorování 4.25. *F je zobrazení* $\iff (\forall x \in \mathrm{Dom}(F))(\exists! y \in \mathrm{Rng}(F))(F(x) = y)$.

Definice 4.26 (Prosté zobrazení, bijekce)**.** Řekneme, že zobrazení F je

- *prosté*, pokud je F^{-1} také zobrazení,

- zobrazení třídy X *do* třídy Y pokud $\mathrm{Dom}(F) = X$ a zároveň $\mathrm{Rng}(F) \subseteq Y$, píšeme $F : X \to Y$,
- zobrazení třídy X *na* třídu Y, pokud $F : X \to Y$ a zároveň $\mathrm{Rng}(F) = Y$,
- *bijekce* mezi třídami X a Y, pokud je to prosté zobrazení X na Y.

Poznámka. Prostým zobrazením se také říká *injekce*, a zobrazením které jsou 'na' se také říká *surjekce*.

Pozorování 4.27. *Pokud je F prosté, potom je F^{-1} také prosté.*

Lemma 4.28. *Pokud je f zobrazení a* $\mathrm{Dom}(f)$ *množina, potom f je také množina.*

Důkaz. Axiom nahrazení nám říká, že zobrazení zobrazují množiny na množiny, tedy $f[\mathrm{Dom}(f)] = \mathrm{Rng}(f)$ je množina a z axiomu vydělení je tedy $f \subseteq \mathrm{Dom}(f) \times \mathrm{Rng}(f)$ také množina. □

Definice 4.29 (Třída zobrazení mezi množinami)**.** Pro třídu A a množinu a definujeme třídu všech zobrazení z množiny a do třídy A jako

$$^{a}A \coloneqq \{f \mid f : a \to A\}.$$

Poznámka. Nelze definovat ^{B}A pokud B je vlastní třída, potom by ta zobrazení $f : B \to A$ už byla vlastní třídy. Obměnou f je množina $\Rightarrow \mathrm{Dom}(f)$ je množina.

Pozorování 4.30. *Tohle ještě nemáme pořádně definované, ale pokud jsou A a B konečné množiny, potom* $\left|^{B}A\right| = |A|^{|B|}$.

Příklad. $^{\varnothing}A = \{\varnothing\}$ a $^{a}\varnothing = \varnothing$, ovšem $^{\varnothing}\varnothing = \{\varnothing\}$. $\ldots 0^0 \coloneqq 1.$

Lemma 4.31 (O velikosti třídy zobrazení)**.** *Platí následující.*

(a) *Pro libovolné množiny x, y je ^{x}y množina.*

(b) *Je-li $x \neq \varnothing$ a Y vlastní třída, potom je ^{x}Y vlastní třída.*

Důkaz. První část pomocí axiomu vydělení, druhá pomocí nahrazení.

(a) $f : x \to y$, pak $f \subseteq x \times y$, tedy $f \in \mathcal{P}(x \times y)$, takže $^{x}y \subseteq \mathcal{P}(x \times y)$. Využíváme, že kartézský součin množin je množina.

(b) Pro každé $y \in Y$ definujeme konstantní zobrazení $K_y : x \to Y$ jako $u \mapsto y$, neboli $K_y = x \times \{y\}$. Protože $x \neq \varnothing$, tak pro $y_1 \neq y_2$ je $K_{y_1} \neq K_{y_2}$. Označme $K \coloneqq \{K_y \mid y \in Y\}$. Zřejmě $K \subseteq {}^{x}Y$. Sporem ukážeme, že K je vlastní třída, (takže ^{x}Y taky). Předpokládejme, že K je množina a definujme zobrazení $F : K \to Y, K_y \mapsto y$. Protože předpokládáme, že K je množina, tak z axiomu nahrazení je i Y množina, ale to je spor. □

Definice 4.32 (Vlastnosti relací)**.** Nechť $R \subseteq \mathbf{V} \times \mathbf{V}$ je relace a X třída. Označme $R_X \coloneqq R \restriction X$. Řekneme, že relace R je na třídě X

- *reflexivní*, pokud $\Delta_X \subseteq R$,
- *antireflexivní*, pokud $\Delta_X \cap R = \varnothing$,
- *symetrická*, pokud $R_X = R_X^{-1}$,
- *slabě antisymetrická*, pokud $R_X \cap R_X^{-1} \subseteq \Delta_X$,
- *silně antisymetrická*, pokud $R_X \cap R_X^{-1} = \varnothing$,
- *tranzitivní*, pokud $R_X \circ R_X \subseteq R_X$.

Pozorování 4.33. *Tyto vlastnosti jsou dědičné, neboli platí na každé podtřídě $Y \subseteq X$.*

4.5 Uspořádání

Definice 4.34 (Uspořádání)**.** Relace $R \subseteq \mathbf{V} \times \mathbf{V}$ je na třídě X

- *trichotomická*, pokud $(\forall x,y \in X)(x\,R\,y \vee y\,R\,x \vee x = y)$,
- *ostré uspořádání* pokud je antireflexivní a tranzitivní na X,
- *uspořádání* pokud je reflexivní, slabě antisymetrická a tranzitivní na X,
- *lineární uspořádání* pokud je to trichotomické uspořádání na X.

Poznámka. Pokud chceme zdůraznit, že dané uspořádání není, nebo nemusí být lineární, tak říkáme, že je *částečné.*

Pokud je R uspořádání, tak místo $x\,R\,y$ píšeme $x \leq_R y$. Dále definujme ostré uspořádání $R' \coloneqq R \setminus \mathbf{Id}$. Namísto $x\,R'\,y$ píšeme $x <_R y$.

Poznámka. Jelikož lze z ostrého uspořádání $<_R$ snadno vyrobit $\leq_R$ a naopak, tak nebudeme definovat vlastnosti zvlášť pro ostré a neostré uspořádání, jelikož jedno implicitně definuje to druhé. Ve větách a důkazech budeme používat tu verzi uspořádání, která se nám zrovna bude hodit víc.

Pozorování 4.35. *Každé ostré uspořádání R je silně antisymetrické.*

Důkaz. Kdyby ne, tak existují $x, y \in X$ takové, že $x\,R\,y$ a $y\,R\,x$. Z tranzitivity $x\,R\,x$, což je spor s antireflexibilitou. □

Příklad. Identita není ostré uspořádání, protože není antireflexivní. Identita je uspořádání. Ale ne lineární, protože různé prvky nejsou porovnatelné. Náležení není uspořádání (ani ostré uspořádání), protože není tranzitivní.

Definice 4.36. Nechť R je uspořádání na třídě A a $X \subseteq A$. Prvek $a \in A$ je

- *horní mez* třídy X, pokud $(\forall x \in X)(x \leq_R a)$, ...také *majoranta*
- *maximální prvek* třídy X, pokud $a \in X \wedge (\nexists x \in X)(a <_R x)$,
- *největší prvek* třídy X, pokud $a \in X$ a je to horní mez X,
- *supremum* třídy X, pokud je nejmenší prvek třídy všech horní mezí X.

Největší prvek, resp. supremum značíme $\max_R(X)$, resp. $\sup_R(X)$; pokud existují. Obdobně definujeme *minorantu*, *minimální prvek*, *nejmenší prvek* a *infimum.*

Pozorování 4.37. *Každý největší prvek je maximální. Pokud je R lineární uspořádání, tak maximální prvek je nejvýše jeden a pokud existuje, tak je největší. Největší prvek i supremum je vždy nejvýše jedno.*

Definice 4.38 (Dolní podmnožina)**.** Nechť R je uspořádání na třídě A. Třída $X \subseteq A$ je

- *shora omezená* v A, pokud existuje $a \in A$ horní mez X,
- *dolní podtřída* třídy A, pokud $(\forall x \in X)(\forall a \in A)(a \leq_R x \Rightarrow a \in X)$.

Každý prvek $a \in A$ určuje dolní podtřídu

$$(\leftarrow, a] \coloneqq \{x \mid x \in A \wedge x \leq_R a\}.$$

Pokud dolní podtřída $X \subseteq A$ je ve skutečnosti množinou, tak říkáme, že to je *dolní podmnožina.*

Pozorování 4.39. *Sjednocení dolních podmnožin je dolní podmnožina.*

Pozorování 4.40. *Nechť R je uspořádání na třídě A. Pak pro libovolné $x, y \in A$ platí*

$$x \leq_R y \iff (\leftarrow, x] \subseteq (\leftarrow, y].$$

Čili uspořádání $\subseteq$ na $\mathcal{P}(A)$ je svým způsobem univerzální. Každé uspořádání lze převést na inkluzi.

Nyní definujeme jeden z nejdůležitějších pojmů teorie množin: *dobrá uspořádání.*

Definice 4.41. Řekneme, že uspořádání R je na množině A

- *husté*, pokud $(\forall x, y \in A)\big(x < y \Rightarrow (\exists z \in A)(x < z < y)\big)$,
- *dobré*, pokud každá neprázdná $B \subseteq A$ má nejmenší prvek,
- *úplné*, pokud každá neprázdná, shora omezená $B \subseteq A$ má supremum.

Pokud je $\leq$ lineární, resp. dobré uspořádání množiny A, tak říkáme, že $(A, \leq)$ je *lineárně*, resp. *dobře uspořádaná množina.* Pokud existuje nějaké úplné uspořádání množiny A, tak říkáme, že A je *úplná.*

Pozorování 4.42. *Lineartita, dobrost a úplnost jsou dědičné vlastnosti.*

Pozorování 4.43. *Každé dobré uspořádání je lineární. Kdyby nebylo, tak by existovaly nějaké dva neporovnatelné prvky a množina těchto dvou prvků by neměla nejmenší prvek.*

Vlastnosti známých uspořádání

- $(\mathbb{N}, \leq)$ Přirozená čísla se standardní interpretací $\leq$ je dobře uspořádaná množina. Její nejmenší prvek je nula.
- $(\mathbb{Z}, \leq)$ Standardní uspořádání celých čísel je lineární, ale není dobré, protože vůči $\leq$ neexistuje nejmenší celé číslo.
- $(\mathbb{Z}, \preceq)$ Uspořádání $x \preceq y \iff (|x| < |y|) \vee (|x| = |y| \wedge x \leq y)$ celých čísel je dobré. Toto uspořádání vypadá následovně: $0, -1, 1, -2, 2, -3, 3, \ldots$
- $(\mathbb{Q}, \leq)$ Standardní uspořádání racionálních čísel je lineární a husté, ale není dobré, protože $\mathbb{Q}$ nemá žádný nejmenší prvek vůči $\leq$. Ovšem není těžké sestrojit nějaké dobré uspořádání. Racionální čísla nejsou úplná.
- $(\mathbb{R}, \leq)$ Standardní uspořádání reálných čísel je lineární, husté a úplné. Ale není dobré a v ZF dokonce existenci žádného dobrého uspořádání reálných čísel není možné dokázat.[3]
- $(\mathbb{N}^+, |\,)$ Kladná celá čísla spolu s relací dělitelnosti jsou částečné uspořádání. Toto uspořádání nemá žádný maximální prvek, ale zato má nejmenší prvek, a sice jedničku.
- $(\mathcal{P}(A), \subseteq)$ Potenční množina libovolné množiny A spolu s inkluzí je částečně uspořádaná množina. V tomto uspořádání je prázdná množina $\varnothing$ nejmenší prvek a A největší prvek.
- $(\Sigma^*, \leq_{LEX})$ Lexikografické uspořádání konečných řetězců nad abecedou Σ je dobré uspořádání. Nejmenší prvek je prázdný řetězec.

[3]Tohle dokázal Paul Cohen v roce 1963 pomocí forcingu, a jako důsledek získal, že je konzistentní předpokládat negaci axiomu výběru.

Izomorfismy uspořádání

Definice 4.44 (Izomorfismus)**.** Nechť A_1, A_2 jsou třídy a R_1, R_2 relace. Bijekce $F : A_1 \to A_2$ je *izomorfismus* tříd A_1, A_2 vzhledem k relacím R_1, R_2, pokud

$$(\forall x,y \in A_1)\big((x, y) \in R_1 \iff (F(x), F(y)) \in R_2\big).$$

Nás bude zajímat primárně případ, kdy relace R_1 a R_2 jsou uspořádání. Řekneme, že uspořádané množiny $(A, \leq_R)$ a $(B, \leq_S)$ jsou *izomorfní* pokud existuje izomorfismus A, B vzhledem k $\leq_R$, $\leq_S$.

Příklad. Dalším případem izomorfismu je izomorfismus grafů. Tam jsou třídy A_1 a A_2 množiny vrcholů grafů G_1 a G_2, relace R_1 je relací „být hranou v G_1“ a R_2 je relací „být hranou v G_2“. Potom je bijekce $f : V_1 \to V_2$ izomorfismus grafů $G_1 = (V_1, E_1)$ a $G_2 = (V_2, E_2)$ právě tehdy, když

$$(\forall u,v \in V_1)\big((u, v) \in E_1 \iff (f(u), f(v)) \in E_2\big).$$

4.6 Vlastnosti dobrých uspořádání

Lemma 4.45. *Pokud je $(A, \leq_R)$ dobře uspořádaná množina a $X \subset A$ její vlastní dolní podmnožina, potom existuje jednoznačně určený prvek $x \in A$ takový, že*

$$X = \{y \in A \mid y <_R x\}.$$

Tuto množinu označíme jako $(\leftarrow, x)$.

Důkaz. Definujeme x jako nejmenší prvek (neprázdné) množiny $W \setminus X$. Potom každé $y <_R x$ patří do X, takže $(\leftarrow, x) \subseteq X$. Chceme ještě opačnou inkluzi. Pro spor předpokládejme, že existuje $y \in X$ co není v $(\leftarrow, x)$. Když $y \not<_R x$, pak nutně $x <_R y$ jelikož $x \neq y$ protože $x \notin X$. Ale tohle znamená, že $x \in X$ protože X je dolní podmnožina a $y \in X$. Spor. □

Definice 4.46 (Počáteční úsek)**.** Pokud $(A, \leq_R)$ je dobře uspořádaná množina, potom jejím vlastním dolním podmnožinám raději říkáme *počáteční úseky*. Počáteční úsek určený prvkem $x \in A$ značíme jako

$$(\leftarrow, x) \coloneqq \{y \in A \mid y <_R x\}.$$

Obsahuje všechny prvky množiny A od jejího minima po x, ale už ne samotné x.

Věta 4.47 (O porovnávání dobrých uspořádání)**.** *Pokud $(A, \leq_R)$ a $(B, \leq_S)$ jsou dobře uspořádané množiny, pak nastane právě jeden ze tří následujících případů:*

(a) *buď A a B jsou izomorfní, nebo*

(b) *A je izomorfní nějakému počátečnímu úseku B, nebo*

(c) *B je izomorfní nějakému počátečnímu úseku A.*

V každém případě je ten izomorfismus určen jednoznačně.

Pro dokázání této věty se nám bude hodit následující definice:

Definice 4.48 (Počátkové vnoření)**.** Nechť $(A, \leq_R)$ a $(B, \leq_S)$ jsou uspořádané množiny. Zobrazení F je *počátkové vnoření* A do B, pokud

(i) $A' \coloneqq \mathrm{Dom}(F) \subseteq A$ je dolní podmnožina A vůči $\leq_R$,

(ii) $B' \coloneqq \mathrm{Rng}(F) \subseteq B$ je dolní podmnožina B vůči $\leq_S$,

(iii) F je izomorfismus A' a B', vzhledem k R a S, tedy

$$(\forall a_1{,}a_2 \in A_D)\big(a_1 \leq_R a_2 \iff F(a_1) \leq_S F(a_2)\big).$$

Tedy F je izomorfismus nějakých dolních podmnožin A a B.

Lemma 4.49. *Nechť F a G jsou počátková vnoření dobře uspořádané množiny $(A, \leq_R)$ do dobře uspořádané množiny $(B, \leq_S)$. Pak buď $F \subseteq G$ nebo $G \subseteq F$.*

Důkaz. Jelikož $\mathrm{Dom}(F)$ i $\mathrm{Dom}(G)$ jsou dolní podmnožiny A, a R je lineární, tak buď $\mathrm{Dom}(F) \subseteq \mathrm{Dom}(G)$, nebo naopak. BÚNO nechť $\mathrm{Dom}(F) \subseteq \mathrm{Dom}(G)$. Zřejmě $F, G \subseteq A \times B$, takže stačí dokázat, že

$$x \in \mathrm{Dom}(F) \implies F(x) = G(x).$$

Pro spor nechť to neplatí a definujme

$$W \coloneqq \{x \in \mathrm{Dom}(F) \mid F(x) \neq G(x)\}.$$

Protože R je dobré, tak existuje $w \coloneqq \min_R(W)$. Jelikož $F(w) \neq G(w)$, tak z linearity S nastane buď $F(w) <_S G(w)$ nebo $G(w) <_S F(w)$, BÚNO nechť platí

$$F(w) <_S G(w). \tag{4.1}$$

Ukážeme, že $F(w) \notin \mathrm{Rng}(G)$, takže $\mathrm{Rng}(G)$ není dolní podmnožina B, což je spor. Pro libovolné $z \in \mathrm{Dom}(G)$ nastane jedna ze dvou situací:

(a) $z <_R w$, z čehož $G(z) <_S F(w)$, protože

$$\begin{aligned} G(z) &= F(z), && w \text{ je nejmenší, pro který se nerovnají} \\ F(z) &<_S F(w). && F \text{ je izomorfismus} \end{aligned}$$

(b) $w \leq_R z$, z čehož $F(w) <_S G(z)$, protože

$$\begin{aligned} F(w) &<_S G(w), && \text{podle (4.1)} \\ G(w) &\leq_S G(z). && G \text{ je izomorfismus} \end{aligned}$$

V každém případě $F(w) \neq G(z)$, tedy $F(w) \notin \mathrm{Rng}(G)$. □

Větu 4.47 můžeme pomocí počátkových vnoření ekvivalentně formulovat takto: Pokud jsou $(A, \leq_R)$ a $(B, \leq_S)$ dobře uspořádané množiny, tak existuje právě jedno zobrazení F, které je počátkové vnoření A do B a navíc nastane alespoň jedno z $\mathrm{Dom}(F) = A$ nebo $\mathrm{Rng}(F) = B$.

Důkaz Věty 4.47. Označme jako P množinu všech počátkových vnoření A do B. Tvrdíme, že $F \coloneqq \bigcup P$ je to hledané zobrazení. Ověříme všechny podmínky:

(1) F je zobrazení. Když $(x, y_1), (x, y_2) \in F$, tak existují počátková vnoření $F_1, F_2 \in P$ taková, že $(x, y_1) \in F_1$ a $(x, y_2) \in F_2$. Podle Lemma 4.49 platí $F_1 \subseteq F_2$ nebo $F_2 \subseteq F_1$. V každém případě jsou obě ty dvojce v alespoň jednom z F_1 nebo F_2, ale protože to jsou zobrazení, tak musí být $y_1 = y_2$.

(2) F je prosté. Podobně, jenom využijeme, že F_1 a F_2 jsou počátková vnoření, tedy izomorfismy, tedy bijekce, takže jsou prosté, z čehož $x_1 = x_2$.

(3) F je počátkové vnoření.

   (i) $\mathrm{Dom}(F)$ je dolní podmnožina A. Nechť $x \in \mathrm{Dom}(F)$, $y \in A$ a $y <_R x$. Potřebujeme ukázat, že $y \in \mathrm{Dom}(F)$. Jelikož $x \in \mathrm{Dom}(F)$, tak existuje nějaké počátkové vnoření $F' \in P$ takové, že $x \in \mathrm{Dom}(F')$. Protože $\mathrm{Dom}(F')$ je dolní podmnožina, tak $y \in \mathrm{Dom}(F') \subseteq \mathrm{Dom}(F)$.

   (ii) $\mathrm{Rng}(F)$ je dolní podmnožina B. Úplně stejná argumentace.

   (iii) F je izomorfismus. Nejprve si uvědomme, že protože je F prosté, tak je to bijekce mezi množinami $\mathrm{Dom}(F)$ a $\mathrm{Rng}(F)$. Nyní nechť $x, y \in \mathrm{Dom}(F)$, potřebujeme aby
$$x \leq_R y \iff F(x) \leq_S F(y).$$
   Opět musí existovat nějaké $F' \in P$ takové, že $y \in \mathrm{Dom}(F')$. F' je počátkové vnoření, takže $\mathrm{Dom}(F')$ je dolní podmnožina, tedy $x \in \mathrm{Dom}(F')$. Navíc, protože je F' izomorfismus, tak
$$F(x) = F'(x) \leq_S F'(y) = F(y).$$

(4) $\mathrm{Dom}(F) = A$ nebo $\mathrm{Rng}(F) = B$. Pro spor nechť $A \setminus \mathrm{Dom}(F)$ i $B \setminus \mathrm{Rng}(F)$ jsou neprázdné. Tedy mají nejmenší prvky a, b. Všimněme si, že $F' := F \cup \{(a, b)\}$ je také počátkové vnoření, tedy $F' \in P$, což je spor. Proč je to počátkové vnoření? Protože $\mathrm{Dom}(F)$ je dolní podmnožina A, tak všechny prvky v $A \setminus \mathrm{Dom}(F)$ musí být větší než všechno v $\mathrm{Dom}(F)$. Tedy a bude nový největší prvek v $\mathrm{Dom}(F')$. Podobně pro b a izomorfismus.

(5) Jednoznačnost. Pro spor nechť existují dvě taková zobrazení $F_1 \neq F_2$. Podle Lemma 4.49 nechť BÚNO $F_1 \subseteq F_2$. Protože $F_1 \neq F_2$, tak existuje nějaké $(a, b) \in F_2 \setminus F_1$. Jenže potom pro F_1 nemůže platit (4), což je spor. □

4.7 Ekvivalence a kvaziuspořádání

Definice 4.50. Relace $R \subseteq \mathbf{V} \times \mathbf{V}$ je na třídě X

- *kvaziuspořádání* pokud je reflexivní a tranzitivní na X,
- *ekvivalence* pokud je reflexivní, symetrická a tranzitivní na X.

Definice 4.51 (Třídy ekvivalence)**.** Nechť R je ekvivalence na třídě X. Pro $x \in X$ definujeme třídu
$$[x]_R := \{y \mid y \in X \wedge x \, R \, y\} = R[\{x\}] \cap X,$$
kterou nazýváme *ekvivalenční třída* prvku x. Pokud je X množina, tak z axiomu vydělení je $[x]_R$ také množina. V tom případě definujeme *množinu ekvivalenčních tříd* množiny X podle ekvivalence R jako
$$X/R := \{[x]_R \in \mathcal{P}(X) \mid x \in X\}.$$

Definice 4.52. *Rozklad množiny* X je libovolná množina $\mathcal{R} \subseteq \mathcal{P}(X)$ splňující

(i) $(\forall a \in \mathcal{R})(a \neq \varnothing)$,

(ii) $(\forall a, b \in \mathcal{R})(a \neq b \Rightarrow a \cap b = \varnothing)$,

(iii) $\bigcup \mathcal{R} = X$.

Lemma 4.53. *Pokud je $\sim$ ekvivalence na množině X, potom je $X/{\sim}$ rozklad X.*

Důkaz. Musíme ukázat, že $X/\sim$ splňuje definici rozkladu.

(i) Z reflexivity $x \sim x$, tedy $x \in [x]$ pro každé $[x] \in X/\sim$.

(ii) Obměnou: ukážeme $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$. Chceme ukázat, že pokud existuje $t \in [x] \cap [y]$ a $a \in [x]$, potom $a \in [y]$. Víme, že $a \sim x$, $x \sim t$, $t \sim y$ a tudíž z tranzitivity $a \sim y$. Použili jsme i symetrii.

(iii) Stačí ukázat, že pokud $x \in X$, potom existuje $a \in X/\sim$ takové, že $x \in a$. Ale toto a je prostě $[x]$. ☐

Pozorování 4.54. *Pokud je relace $\lesssim$ kvaziuspořádání na množině X, potom můžeme definovat ekvivalenci $\sim$ na X předpisem*

$$x \sim y \iff x \lesssim y \wedge y \lesssim x.$$

Potom můžeme definovat uspořádání $\leq$ na množině $X/\sim$ jako

$$[x]_\sim \leq [y]_\sim \iff x \lesssim y.$$

Tato konstrukce je velmi šikovná, často se totiž potýkáme s množinou X, která je skoro uspořádaná relací R, až na to, že R není antisymetrická na některých podmnožinách X. Potom prostě prohlásíme tyto zlobivé prvky za ekvivalentní a definujeme nové uspořádání na třídách ekvivalence.

Ovšem pokud je X vlastní třída, tak to nemusí fungovat. Může se stát, že pro nějaké $x \in X$ bude $[x]_\sim$ také vlastní třída, a potom nelze definovat $X/\sim$.

5 Porovnávání mohutností množin

Definice 5.1. Pro množiny x a y definujeme relace

(a) $x \approx y$, pokud existuje bijekce $f : x \to y$,

(b) $x \preceq y$, pokud existuje prosté zobrazení $f : x \to y$,

(c) $x \prec y$, pokud $x \preceq y$ a zároveň $x \not\approx y$.

Poznámka. Pro třídy tato definice nemá smysl, protože by nešlo kvantifikovat f.

Poznámka. Relaci $x \preceq y$ jsme také mohli definovat jako „existuje zobrazení y na x“. Ale potom by Věta 5.5 nešla dokázat bez AC. Důvod je následující:

Platí, že existuje-li prosté zobrazení x do y, potom existuje zobrazení y na x. Prostě vezmu ten jednoznačně určený prvek. Ale opačný směr bez AC neplatí, protože se na jeden prvek může zobrazit nekonečně mnoho prvků a tohle se může stát nekonečně-mnoho krát, takže to prosté zobrazení v opačném směru bez AC nesestrojím (nemám jak *vybrat* ty prvky).

Pozorování 5.2. *Pro libovolné množiny x, y, z platí*

- $x \subseteq y \implies x \preceq y$,
- $x \subset y \implies x \preceq y$, *. . . ale ne $x \prec y$*
- $x \approx x$, *. . . identitou*
- $x \approx y \implies y \approx x$, *. . . inverzní bijekcí*
- $(x \approx y \wedge y \approx z) \implies x \approx z$, *. . . složení bijekcí je bijekce*
- $x \preceq x$, *. . . identitou*
- $(x \preceq y \wedge y \preceq z) \implies x \preceq z$, *. . . složení prostých zobrazení je prosté*

Důsledek 5.3. *Relace $\approx$ je ekvivalence a relace $\preceq$ je kvaziuspořádání. Ale ne uspořádání, protipříklad na antisymetrii je třeba $\{\varnothing\}$ a $\{\{\varnothing\}\}$.*

Je dobré se zeptat, zda lze $\preceq$ převést na uspořádání ekvivalenčních tříd $[x]_\approx$? Bohužel ne, protože to jsou vlastní třídy, takže $\mathbf{V}/\approx$ neexistuje. Kdyby pro nějaké $x \neq \varnothing$ byla $[x]_\approx$ množinou, tak $\mathbf{V} = \bigcup [x]_\approx$ by také byla množinou.

Co ale udělat lze, a je to velmi důležité, je definovat určité kanonické reprezentanty těchto ekvivalenčních tříd, kterým se říká *kardinální čísla.* Z axiomu výběru[4] pak plyne, že pro každou množinu x existuje právě jedno kardinální číslo κ takové, že $x \approx \kappa$. *Mohutnost* nebo *kardinalitu* množiny x potom definujeme jako $|x| := \kappa$. Tomuto konceptu se budeme více věnovat v Sekci 9.

Lemma 5.4. *Nechť x, y, x_1, y_1 a z jsou množiny. Pak*

(1) $x \times y \approx y \times x$,

(2) $x \times (y \times z) \approx (x \times y) \times z$,

(3) $(x \approx x_1 \wedge y \approx y_1) \implies (x \times y) \approx (x_1 \times y_1)$,

(4) $x \approx y \implies \mathcal{P}(x) \approx \mathcal{P}(y)$,

[4] Konečná kardinální čísla jsou právě přirozená čísla, a pro ty axiom výběru potřeba není, jak ukážeme v důkazu Věty 5.42.

(5) $\mathcal{P}(x) \approx {}^{x}2$. $\quad \ldots 2 = \{0,1\} = \{\varnothing, \{\varnothing\}\}$

Důkaz. Vždy sestrojíme nějakou bijekci h.

(1) $h : (u,v) \mapsto (v,u)$,

(2) $h : (a,(b,c)) \mapsto ((a,b),c)$,

(3) $f : x \to x_1$ a $g : y \to y_1$. Uděláme $h : (a,b) \mapsto (f(a), g(b))$,

(4) $f : x \to y$. Uděláme $h : u \mapsto f[u]$,

(5) Pro $u \subseteq x$ definujeme charakteristickou funkci $\chi_u : x \to \{0,1\}$ předpisem

$$\chi_u(a) := \begin{cases} 1, & a \in u, \\ 0, & a \notin u. \end{cases}$$

Bijekci $h : \mathcal{P}(x) \to {}^{x}2$ definujeme jako $h : u \mapsto \chi_u$. □

5.1 Cantor–Schröder–Bernsteinova věta

Dokážeme, že naše definice pro srovnávání velikostí množin dává dobrý smysl.

Věta 5.5 (Cantor, Schröder, Bernstein)**.** *$x \approx y \iff (x \preceq y \wedge y \preceq x)$.*

Tuto větu lze dokázat více způsoby; my ji získáme jako důsledek obecnějšího tvrzení, hovořícího o pevných bodech určitých funkcí.

Definice 5.6 (Monotónní zobrazení)**.** Zobrazení $H : \mathcal{P}(x) \to \mathcal{P}(y)$ je *monotónní vzhledem k inkluzi*, pokud pro všechny $u,v \subseteq x$ platí

$$u \subseteq v \Rightarrow H(u) \subseteq H(v).$$

Lemma 5.7 (O pevném bodu)**.** *Je-li $H : \mathcal{P}(x) \to \mathcal{P}(x)$ monotónní vzhledem k inkluzi, pak existuje $c \in \mathcal{P}(x)$ takové, že $H(c) = c$.*

Intuice. Představme si na chvíli, že H je funkce reálných čísel a chceme najít její pevný bod. Potom dává smysl podívat se na množinu $\{x \mid x \leq H(x)\}$. Nemělo by nás překvapit, kdyby supremum této množiny byl pevný bod. Ale co je supremum v našem kontextu? Když uspořádáme $A \subseteq \mathcal{P}(x)$ pomocí $\subseteq$, pak $\sup_{\subseteq}(A) = \bigcup A$.

Důkaz. Nechť $A := \{u \in \mathcal{P}(x) \mid u \subseteq H(u)\}$ a označme $c := \sup_{\subseteq}(A) = \bigcup A$. Ukážeme, že $H(c) = c$. Pro každou $u \in A$ platí

$$\begin{aligned} u &\subseteq c, && c \text{ je horní mez } A && (5.1)\\ u &\subseteq H(u), && u \in A \\ H(u) &\subseteq H(c), && H \text{ je monotónní} \\ u &\subseteq H(c). && \text{z předchozích dvou} \end{aligned}$$

Tedy $H(c)$ je horní mez A. Protože c je nejmenší horní mez A, tak platí

$$\begin{aligned} c &\subseteq H(c), && c \text{ je supremum } A \\ H(c) &\subseteq H(H(c)), && H \text{ je monotónní} && (5.2)\\ H(c) &\in A, && \text{podle (5.2)} \\ H(c) &\subseteq c. && \text{podle (5.1)} \end{aligned}$$

Máme inkluzi v obou směrech, takže $c = H(c)$. □

Důkaz Věty 5.5. Směr '$\Rightarrow$' je triviální. Pro '$\Leftarrow$' nechť $f : x \to y$ a $g : y \to x$ jsou prostá zobrazení. Uvažme „indukovaná" zobrazení

$$\begin{aligned} \mathbf{f} : \mathcal{P}(x) &\to \mathcal{P}(y) & \qquad \mathbf{g} : \mathcal{P}(y) &\to \mathcal{P}(x) \\ u &\mapsto f[u], & v &\mapsto g[v]. \end{aligned}$$

Například $\mathbf{f}(\{1,2,3\}) = \{f(1), f(2), f(3)\}$. Všimněme si, že $\mathbf{f}$ i $\mathbf{g}$ jsou monotónní vzhledem k inkluzi. Chceme zobrazit kus x pomocí $\mathbf{f}$ na kus y a zbytek y zobrazit pomocí $\mathbf{g}$ zpátky na zbytek x. Ale obecně to nemusí dohromady vyplnit celou množinu x a můžou tam být nějaké duplicity.

Definujme zobrazení $H : \mathcal{P}(x) \to \mathcal{P}(x)$ jako $H : u \mapsto x - \mathbf{g}(y - \mathbf{f}(u))$. Dělá to, co je popsané výše a na konci vezme doplněk. Naším cílem je najít nějaké $c \subseteq x$, aby $H(c) = c$, tedy c a $\mathbf{g}(y - \mathbf{f}(c))$ tvoří rozklad x. Stačí ukázat, že H je monotónní vzhledem k inkluzi. Vezměme libovolné $u \subseteq v \subseteq x$. Máme

$$\begin{aligned} \mathbf{f}(u) &\subseteq \mathbf{f}(v), && \mathbf{f} \text{ je monotónní} \\ y - \mathbf{f}(u) &\supseteq y - \mathbf{f}(v), && \text{doplněk do } y \\ \mathbf{g}(y - \mathbf{f}(u)) &\supseteq \mathbf{g}(y - \mathbf{f}(v)), && \mathbf{g} \text{ je monotónní} \\ H(u) &\subseteq H(v). && \text{doplněk do } x \end{aligned}$$

Podle Lemma 5.7 má H pevný bod, označme jej c. Tedy $c = x - \mathbf{g}(y - \mathbf{f}(c))$, takže $g[y - \mathbf{f}(c)] = x - c$. To znamená, že restrikce $g \restriction (y - \mathbf{f}(c))$ je prosté zobrazení $y - \mathbf{f}(c)$ na $x - c$, čili bijekce. Inverze bijekce je opět bijekce, tedy $g^{-1} \restriction (x - c)$ je bijekce mezi $x - c$ a $y - f[c]$. To doplníme bijekcí $f \restriction c$ mezi c a $f[c]$, čímž získáme bijekci $h \coloneqq (f \restriction c) \cup (g^{-1} \restriction (x - c))$ mezi x a y, kterou také lze zapsat jako

$$h(a) = \begin{cases} f(a), & a \in c, \\ g^{-1}(a), & a \in x - c. \end{cases}$$

Můžeme tedy prohlásit, že $x \approx y$. $\square$

5.2 Definice přirozených čísel a množiny ω

Zermelo chtěl přirozená čísla definovat jako $0 \coloneqq \varnothing$ a $n \coloneqq \{n-1\}$. Russel a Frege zase jako $n \coloneqq \{x \mid x \text{ má } n \text{ prvků}\}$, to jsou ale vlastní třídy. Dnes se používá definice, kterou navrhl Von Neumann:

$$0 \coloneqq \varnothing,\ 1 \coloneqq \{0\},\ 2 \coloneqq \{0,1\},\ \ldots,\ n+1 \coloneqq \{0,1,\ldots,n\} = n \cup \{n\}.$$

Definice 5.8. *Funkci následníka* $\mathcal{S} : \mathbf{V} \to \mathbf{V}$ je definovaná jako $v \mapsto v \cup \{v\}$. Pro větší pohodlnost zápisu budeme namísto $\mathcal{S}(v)$ občas psát $v + 1$.

Definice 5.9. Množina w je *induktivní* pokud $0 \in w$ a pro všechna $n \in w$ také $n + 1 \in w$.

Axiom 5.10 (Axiom nekonečna)**.** Existuje nějaká induktivní množina.

Definice 5.11. Množina všech přirozených čísel je $\omega \coloneqq \bigcap\{w \mid w \text{ je induktivní}\}$.

Lemma 5.12. *ω je nejmenší induktivní množina (vzhledem k inkluzi).*

Důkaz. Pokud je w induktivní, tak $0 \in w$, takže $0 \in \omega$. Pokud $n \in \omega$, tak pro všechny induktivní množiny w také $n \in w$, tedy i $n + 1 \in w$ a tudíž $n + 1 \in \omega$. $\square$

Tvrzení 5.13. $\omega \approx \omega \times \omega$.

Důkaz. Využijeme Větu 5.5 a definujeme prostá zobrazení

$$\begin{aligned} f : \omega &\to \omega \times \omega \qquad\qquad & g : \omega \times \omega &\to \omega \\ n &\mapsto (n, 0), & (a, b) &\mapsto 2^a \cdot 3^b. \end{aligned}$$

Zobrazení g je prosté ze základní věty aritmetiky. □

Úloha 5.14. Ukažte, že $\omega \approx \mathbb{Q}$, kde $\mathbb{Q}$ značí množinu všech racionálních čísel.

Nápověda. Zlomky jsou vlastně uspořádané trojice $\mathbb{Q} \subseteq \omega \times \omega \times 2$. Například $-3/4$ odpovídá trojici (3,4,1) nebo 4/8 trojici (4,8,0).

Princip indukce pro přirozená čísla

Věta 5.15. *Pokud je podmnožina $X \subseteq \omega$ induktivní, potom $X = \omega$.*

Důkaz. Z definice ω platí $\omega \subseteq X$, tedy máme inkluzi v obou směrech. □

Známé využití tohoto principu je následující. Řekněme, že chceme dokázat že všechna přirozená čísla $n \in \omega$ mají nějakou vlastnost $\varphi(n)$. Pak dokážeme

$$\varphi(0) \quad \wedge \quad (\forall n \in \omega)\big(\varphi(n) \Rightarrow \varphi(n+1)\big),$$

a podle principu indukce $X \coloneqq \{n \in \omega \mid \varphi(n)\} = \omega$.

Úloha 5.16. Dokažte z Tvrzení 5.13 indukcí, že $\omega \approx \omega^n$ pro každé $0 \neq n \in \omega$.

5.3 Konečné množiny

Chtěli bychom nějak vyjádřit, co to znamená, že daná množina je konečná. Asi nejpřirozenější je říct, že množina x je konečná, pokud existuje nějaké přirozené číslo n takové, že $x \approx n$. My to uděláme trochu oklikou a zavedeme poněkud méně intuitivní definici, která se ale ukáže být šikovná v důkazech. Posléze ukážeme, že tyto dvě definice jsou ve skutečnosti ekvivalentní.

5.3.1 Definice konečnosti

Definice 5.17 (Tarski)**.** Množina x je *konečná*, pokud každá neprázdná $a \subseteq \mathcal{P}(x)$ má maximální prvek vůči inkluzi. Pokud je x konečná, tak píšeme $\mathrm{Fin}(x)$.

Tohle by pro konečné množiny mělo intuitivně platit. Vyberu nějaký prvek. Pokud je maximální, vyhrál jsem. Pokud není, existuje větší prvek, vyberu jej a opakuji. Ale třeba pro množinu všech přirozených čísel ω to už neplatí. Když označíme $[n] \coloneqq \{1, 2, \dots, n\}$, tak množina $\{[n] \mid n \in \omega\} \subseteq \mathcal{P}(\omega)$ nemá maximální prvek. Tento argument zformalizujeme později.

Pozorování 5.18. *Množina x je konečná $\iff$ každá neprázdná $a \subseteq \mathcal{P}(x)$ má minimální prvek vůči inkluzi.*

Důkaz. Definujeme $d : \mathcal{P}(x) \to \mathcal{P}(x), u \mapsto x \setminus u$. Potom $u \subseteq v \Leftrightarrow d(u) \supseteq d(v)$. Klíčová úvaha: v je maximum množiny $a \subseteq \mathcal{P}(x)$ právě tehdy, když $d(v)$ je minimum množiny $d[a] = \{d(u) \mid u \in a\}$. □

Ověříme, že konečné množiny jsou menší než ty nekonečné.

Lemma 5.19. *Je-li x konečná a y nekonečná, potom $x \prec y$.*

Důkaz. Pro spor nechť $y \preceq x$, tedy existuje prosté zobrazení $f : y \to x$. Jelikož y je nekonečná, tak existuje $\varnothing \neq u \subseteq \mathcal{P}(y)$, která nemá maximální prvek vůči inkluzi. Definujme zobrazení $g : \mathcal{P}(y) \to \mathcal{P}(x)$ jako $g : a \mapsto f[a]$. Nyní množinu $u \subseteq \mathcal{P}(y)$ zobrazíme na množinu $g[u] \subseteq \mathcal{P}(x)$. Protože je x konečná, tak $g[u]$ má maximální prvek vůči inkluzi, označme jej m. Zobrazme nyní m pomocí g^{-1} zpátky do u, čímž získáme $n_0 := g^{-1}(m) \in u$. Jelikož u nemá maximální prvek vůči inkluzi, tak existuje $n_1 \in u$ takové, že $n_0 \subset n_1$. Jelikož je f prostá, tak jsou g a g^{-1} také prosté, a proto $m = g(n_0) \subset g(n_1)$, což je spor s maximalitou m. □

Dedekindova definice konečnosti Uvedeme ještě jednu poměrně přirozenou definici konečnosti.

Definice 5.20. Množina x je *dedekindovsky konečná*, pokud $y \prec x$ pro všechny vlastní podmnožiny $y \subset x$. Množiny bez této vlastnosti jsou *dedekindovsky nekonečné*.

Lemma 5.21. *Je-li x konečná, potom je i dedekindovsky konečná.*

Důsledek 5.22. *Je-li x dedekindovsky nekonečná, potom je nekonečná.*

Důkaz. Pro spor nechť pro nějaké $y \subset x$ platí $y \approx x$ a definujeme množinu všech takových zlobivých y jako

$$A := \{y \subset x \mid y \approx x\}.$$

Protože $A \neq \varnothing$ a $A \subseteq \mathcal{P}(x)$, tak z konečnosti x existuje c, minimální prvek A vůči inkluzi. Protože $x \approx c$, tak existuje bijekce $f : x \to c$. Označme $d := f[c]$. Protože $c \subset x$, tak $f[c] \subset f[x]$, tedy $d \subset c$. Jenže $f \restriction c$ je bijekce mezi c a d, tedy $c \approx d$, z čehož $d \approx x$, tedy $d \in A$. To je spor s minimalitou c. □

Poznámka. Opačná implikace v ZF dokázat nelze, potřebujeme alespoň nějakou slabou variantu axiomu výběru. V ZF dokonce mohou existovat dedekindovsky konečné množiny x, pro které je $\mathcal{P}(x)$ dedekindovsky nekonečná.

Tvrzení 5.23. *ω je dedekindovsky nekonečná, a tedy nekonečná.*

Důkaz. Musíme najít nějakou množinu $w \subset \omega$ takovou, že $w \approx \omega$. Vezměme množinu $w := \omega \setminus \{0\}$. Naší bijekcí je funkce následníka $S : \omega \to w$, $n \mapsto n + 1$. □

Další definice konečnosti Přestože Dedekindova definice konečnosti není ekvivalentní Tarskiho definici, existuje spousta jiných tvrzení, které jí ekvivalentní jsou:

Fakt 5.24. *Následující tvrzení jsou ekvivalentní:*

(1) *Množina x je konečná (podle Tarskiho).*

(2) *Existuje nějaké $n \in \omega$ takové, že $x \approx n$.*

(3) *Existuje lineární uspořádání '$\leq$' na x, které je dobré, a '$\geq$' je také dobré.*

(4) *Existuje nějaké lineární uspořádání na x, a navíc každá dvě lineární uspořádání na x jsou izomorfní.*

(5) *$\mathcal{P}(\mathcal{P}(x))$ je dedekindovsky konečná.*

5.3.2 Vlastnosti konečných uspořádání

Lemma 5.25. *Je-li x konečná množina uspořádaná relací $\leq$, potom má každá neprázdná $y \subseteq x$ minimální i maximální prvek vůči $\leq$.*

Důkaz. Maximalitu vůči $\leq$ převedeme na maximalitu vůči $\subseteq$. Máme $(x, \leq)$ a $\varnothing \neq y \subseteq x$. Pro každé $a \in y$ uvažme $(\leftarrow, a] \subseteq x$. Označme $u \coloneqq \{(\leftarrow, a] \mid a \in y\} \subseteq \mathcal{P}(x)$. Jelikož $u \neq \varnothing$ a x je konečná, tak u má minimální i maximální prvek vůči inkluzi. Všimněme si, že pokud je $(\leftarrow, m]$ maximální v u vzhledem k $\subseteq$, tak m je maximální v y vzhledem k $\leq$. Obdobně pro minimum. $\square$

Důsledek 5.26. *Každé lineární uspořádání na konečné množině je dobré.*

Důkaz. Jelikož v lineárním uspořádání je minimální prvek automaticky i nejmenší. $\square$

Věta 5.27. *Každá dvě lineární uspořádání na konečné množině jsou izomorfní.*

Důkaz. Nechť R, S jsou lineární uspořádání na konečné množině x. Protože x je konečná, tak díky předchozímu důsledku to jsou dokonce dobrá uspořádání. Máme tedy dvě dobře uspořádané množiny, $(x, \leq_R)$ a $(x, \leq_S)$. Podle Věty 4.47 je množina $(x, \leq_R)$ izomorfní s nějakou dolní podmnožinou $(y, \leq_S) \subseteq (x, \leq_S)$. Mohlo by to být i naopak, ale BÚNO uvažme tuto variantu. Chceme ukázat, že $y = x$. Pro spor nechť $y \subset x$. Jelikož se jedná o izomorfismus, tedy speciálně bijekci, tak $y \approx x$. Což ale znamená, že x není dedekindovsky konečná, a to je spor s Lemma 5.21. $\square$

5.3.3 Princip indukce pro konečné množiny

Definice 5.28. Definujeme třídu všech konečných množin $\mathrm{Fin} \coloneqq \{x \mid \mathrm{Fin}(x)\}$

Věta 5.29 (Princip indukce pro konečné množiny). *Je-li X třída, pro kterou platí*

(i) $\varnothing \in X$,

(ii) $x \in X \Rightarrow (\forall y)(x \cup \{y\} \in X)$,

potom $\mathrm{Fin} \subseteq X$.

Důkaz. Pro spor nechť existuje nějaká množina $x \in \mathrm{Fin} \setminus X$. Definujme

$$w \coloneqq \{v \subseteq x \mid v \in X\}.$$

Podle (i) je $\varnothing \in w$, takže $\varnothing \neq w \subseteq \mathcal{P}(x)$. Protože je x konečná, tak w má maximální prvek vůči inkluzi, označme jej v_0. Tedy $v_0 \subseteq x$, ale $v_0 \neq x$, protože $v_0 \in X$. To znamená, že existuje nějaký prvek $y \in x \setminus v_0$. Položme $v_1 \coloneqq v_0 \cup \{y\}$. Podle (ii) platí $v_1 \in w$, což je spor s maximalitou v_0. $\square$

Fakt 5.30. *Tvrzení že relace porovnávání velikostí množin $\preceq$ je trichotomická na $\mathbf{V}$, je ekvivalentní axiomu výběru, čili jej v* ZF *nelze dokázat.*

Ukážeme, že pro konečné množiny to jde:

Lemma 5.31. *Každá konečná množina je srovnatelná se všemi množinami.*

$$\mathrm{Fin}(x) \implies (\forall y)(x \preceq y \vee y \preceq x).$$

Důkaz. Pomocí principu indukce. Ukážeme, že $X \coloneqq \{x \mid (\forall y)(x \preceq y \vee y \preceq x)\}$ splňuje obě dvě podmínky, z čehož $\mathrm{Fin} \subseteq X$ a platí to pro všechny konečné množiny.

(i) $\varnothing \in X$ protože $(\forall y) : \varnothing \subseteq y$, takže $\varnothing \preceq y$.

(ii) Nechť $x \in X$, u je libovolná množina a $z = x \cup \{u\}$. Chceme ukázat, že $z \in X$. BÚNO $u \notin x$. Nechť y je libovolná množina. Podle předpokladu je $x \preceq y$ nebo $y \preceq x$. Mohou nastat dvě možnosti:

  (a) $y \preceq x$, pak $y \preceq x \cup \{u\}$.

  (b) $x \prec y$, ukážeme $x \cup \{u\} \preceq y$. Nechť $f : x \to y$ je prosté zobrazení x do y. Jelikož $x \prec y$, tak existuje $v \in y \setminus f[x]$. Definujme $g : x \cup \{u\} \to y$ jako $g \coloneqq f \cup (u, v)$. g je prosté zobrazení $x \cup \{u\}$ do y, tedy $x \cup \{u\} \preceq y$. $\square$

Úloha 5.32. Dokažte indukcí, že pokud x je konečná a $f : x \to y$, potom $\mathrm{Rng}(f) \preceq x$.

Úloha 5.33. Dokažte indukcí, že každou konečnou množinu lze dobře uspořádat.

5.3.4 Operace zachovávající konečnost

Lemma 5.34. *Platí*

(a) $\mathrm{Fin}(x) \wedge y \subseteq x \implies \mathrm{Fin}(y)$,

(b) $\mathrm{Fin}(x) \wedge y \approx x \implies \mathrm{Fin}(y)$,

(c) $\mathrm{Fin}(x) \wedge y \preceq x \implies \mathrm{Fin}(y)$.

Důkaz. Všechno to jsou snadná pozorování:

(a) Ukážeme, že libovolná $\varnothing \neq w \subseteq \mathcal{P}(y)$ má maximální prvek. To je jednoduché, protože $w \subseteq \mathcal{P}(y) \subseteq \mathcal{P}(x)$, tudíž $w \subseteq \mathcal{P}(x)$ a x je konečná.

(b) Zřejmě $\mathcal{P}(x) \approx \mathcal{P}(y)$, dokonce jsou izomorfní vzhledem k $\subseteq$. Vynecháme detaily.

(c) Plyne z předchozích dvou. Vezmeme nějakou $z \subseteq x$ takovou, že $z \approx y$. $\square$

Lemma 5.35. $\mathrm{Fin}(x) \wedge \mathrm{Fin}(y) \implies \mathrm{Fin}(x \cup y)$

Důkaz. Nechť $\varnothing \neq w \subseteq \mathcal{P}(x \cup y)$, nalezneme maximální prvek. Idea je taková, že se zvlášť podíváme na x-ové a y-ové prvky množin ve w, najdeme maxima a zkombinujeme je. Definujme zobrazení

$$f_x : w \to \mathcal{P}(x) \qquad\qquad f_y : w \to \mathcal{P}(y)$$
$$u \mapsto u \cap x, \qquad\qquad u \mapsto u \cap y.$$

Potom označme
$$w_x \coloneqq \{f_x(u) \mid u \in w\}.$$

Zřejmě $\varnothing \neq w_x \subseteq \mathcal{P}(x)$, takže má maximální prvek vůči inkluzi, označme jej v_x. Nyní položme
$$w_y \coloneqq \{f_y(u) \mid u \in w \wedge f_x(u) = v_x\}.$$

Opět $\varnothing \neq w_y \subseteq \mathcal{P}(y)$, takže má maximální prvek v_y. Všimněme si, že $v_x \cup v_y$ je hledaný maximální prvek množiny w. Kdyby ne, tak by to byl spor s maximalitou v_x nebo v_y. $\square$

Tvrzení 5.36. *Sjednocení konečně mnoha konečných množin je konečná množina.*

$$\mathrm{Fin}(x) \wedge (\forall a \in x)\, \mathrm{Fin}(a) \implies \mathrm{Fin}\big(\bigcup x\big).$$

Důkaz. Pomocí principu indukce. Položme $X = \{x \mid x \subseteq \mathrm{Fin} \Rightarrow \mathrm{Fin}\big(\bigcup x\big)\}$.

(i) $\varnothing \in X$, protože $\bigcup \varnothing = \varnothing$ a $\mathrm{Fin}(\varnothing)$.

(ii) Nechť $x \in X$, y je libovolná množina, ukážeme $x \cup \{y\} \in X$. Pokud y je nekonečná, tak $x \cup \{y\} \nsubseteq \mathrm{Fin}$. Jinak suma množiny $x \cup \{y\}$ je

$$\bigcup(x \cup \{y\}) = y \cup \bigcup x,$$

tedy sjednocení dvou konečných množin, což je konečná množina. □

Důsledek 5.37 (Dirichletův princip pro nekonečné množiny)**.** *Je-li nekonečná množina sjednocením konečně mnoha množin, pak alespoň jedna z nich je nekonečná.*

Lemma 5.38. $\mathrm{Fin}(x) \implies \mathrm{Fin}(\mathcal{P}(x))$.

Důkaz. Pomocí principu indukce. Položme $X \coloneqq \{x \mid \mathrm{Fin}(\mathcal{P}(x))\}$.

(i) $\varnothing \in X$, protože $\mathcal{P}(\varnothing) = \{\varnothing\}$ je konečná množina.

(ii) Nechť $x \in X$ a y je libovolná množina, ukážeme $x \cup \{y\} \in X$. BÚNO $y \notin x$. Rozdělíme $\mathcal{P}(x \cup \{y\})$ na dvě části: $\mathcal{P}(x)$ a $z \coloneqq \mathcal{P}(x \cup \{y\}) \setminus \mathcal{P}(x)$. Všimněme si, že $\mathcal{P}(x) \approx z$ bijekcí $f : \mathcal{P}(x) \to z, u \mapsto u \cup \{y\}$. Z předpokladu je $\mathcal{P}(x)$ konečná, tedy z konečná také a sjednocení konečných množin je konečné, tedy $\mathcal{P}(x) \cup z = \mathcal{P}(x \cup \{y\})$ je konečná množina. □

Důsledek 5.39. $\mathrm{Fin}(x) \wedge \mathrm{Fin}(y) \implies \mathrm{Fin}(x \times y)$

Důkaz. $x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y))$, jak jsme již ukázali v důkazu Lemma 4.15. □

Úloha 5.40. Ukažte pomocí principu indukce, že kartézský součin konečně mnoha konečných množin je konečný.

5.3.5 Definice konečnosti pomocí přirozených čísel

Vzpomeňme si, že přirozená čísla jsme definovali jako

$$0 \coloneqq \varnothing,\ 1 \coloneqq \{0\},\ 2 \coloneqq \{0, 1\},\ \ldots,\ n + 1 \coloneqq \{0, 1, \ldots, n\} = n \cup \{n\}.$$

Lemma 5.41. *Každé přirozené číslo je konečná množina. Neboli $n \in \omega \Rightarrow \mathrm{Fin}(n)$.*

Důkaz. Indukcí podle n. Zjevně $\mathrm{Fin}(0)$. Nyní nechť pro $n \in \omega$ platí $\mathrm{Fin}(n)$. Protože sjednocení dvou konečných množin je konečné, máme $\mathrm{Fin}(n \cup \{n\})$ □

Věta 5.42. *Množina x je konečná $\iff$ $x \approx n$ pro nějaké $n \in \omega$.*

Důkaz. Směr '$\Leftarrow$' z předchozího lemma. Opačný směr principem indukce pro konečné množiny. Definujeme množinu

$$X \coloneqq \{x \mid (\exists n \in \omega)(x \approx n)\}.$$

Splníme předpoklady principu indukce, z čehož poplyne $\mathrm{Fin}(x) \Rightarrow x \in X$.

(i) $\varnothing \in X$, protože $\varnothing \approx 0$.

(ii) Nechť $x \in X$ a y je množina. Chceme ukázat $x \cup \{y\} \in X$. Máme $x \approx n$ pro nějaké $n \in \omega$. BÚNO nechť $y \notin x$ (jinak $x \cup \{y\} = x \approx n$). Tvrdíme, že $x \cup \{y\} \approx n + 1$. Bijekci $f : x \to n$ rozšíříme o prvek (y, n), čímž získáme bijekci $g : x \cup \{y\} \to n + 1$. Tedy $x \cup \{y\} \approx n + 1$ a $x \cup \{y\} \in X$. □

5.4 Uspořádání přirozených čísel relací náležení

Lemma 5.43 (O vlastnostech přirozených čísel)**.** *Pro libovolná* $n, m \in \omega$ *platí*

(a) $n \in \omega \Rightarrow n \subseteq \omega$,

(b) $m \in n \Rightarrow m \subseteq n$,

(c) $n \notin n$.

Důkaz. Tohle je intuitivně zřejmé, ale my to dokážeme formálně indukcí podle n.

(a) Pro nulu to platí, protože $0 \subseteq \omega$. Potom pro $n \in \omega$ už máme $n \subseteq \omega$. Protože $n \in \omega$, tak $\{n\} \subseteq \omega$ a i $n \cup \{n\} \subseteq \omega$

(b) Pro nulu to zjevně platí. Nyní nechť to platí pro n. Chceme ukázat, že pokud $m \in \mathcal{S}(n)$, potom $m \subseteq \mathcal{S}(n)$. Jelikož $m \in \mathcal{S}(n) = n \cup \{n\}$, tak buď $m \in n$ a z indukčního předpokladu $m \subseteq n \subseteq \mathcal{S}(n)$, nebo $m = n \subseteq \mathcal{S}(n)$.

(c) Pro nulu to platí. Nyní nechť $n \in \omega$ a $n \notin n$. Pro spor předpokládejme, že $\mathcal{S}(n) \in \mathcal{S}(n) = n \cup \{n\}$. Potom buď $\mathcal{S}(n) \in n$ nebo $\mathcal{S}(n) = n$. V obou případech dostáváme inkluzi $\mathcal{S}(n) \subseteq n$. Jenomže $\mathcal{S}(n) = n \cup \{n\}$, takže $n \in n$ což je spor s indukčním předpokladem. □

V Tvrzení 5.23 jsme dokázali, že ω je dedekindovsky nekonečná a tudíž nekonečná. Teď to uděláme přímo z definice konečnosti.

Tvrzení 5.44. *ω je nekonečná.*

Důkaz. Musíme najít nějakou neprázdnou podmnožinu $\mathcal{P}(\omega)$, která nemá maximální prvek. Ukáže se, že to je samotná ω. Podle Lemma 5.43 pro každé $n \in \omega$ platí $n \subseteq \omega$, tedy $n \in \mathcal{P}(\omega)$, proto $\omega \subseteq \mathcal{P}(\omega)$. Zjevně $\omega \neq \emptyset$. Ukážeme, že nemá maximální prvek vůči inkluzi. Když $n \in \omega$, tak $n \subset n \cup \{n\} \in \omega$, tedy n není maximální. □

Lemma 5.45. *Pro libovolná* $n, m \in \omega$ *platí*

$$m \in n \iff m \subset n$$

Důkaz. Směr '$\Rightarrow$' plyne z $m \subseteq n$ a $n \notin n$. Směr '$\Leftarrow$' indukcí podle n. Pro $n = 0$ nelze splnit předpoklad $m \subset 0$, takže to platí. Nyní nechť to platí pro nějaké $n \in \omega$. Předpokládáme, že $m \subset \mathcal{S}(n)$, budeme chtít ukázat, že $m \in \mathcal{S}(n)$.

Ukážeme $m \subseteq n$, tedy buď $m \subset n$ a podle indukčního předpokladu $m \in n$, nebo $m = n$, každopádně $m \in n \cup \{n\} = \mathcal{S}(n)$.

Pro spor nechť $m \subset \mathcal{S}(n) = n \cup \{n\}$, ale $m \nsubseteq n$. Potom musí být $n \in m$, tudíž podle Lemma 5.43 $n \subseteq m$, takže $n \cup \{n\} = \mathcal{S}(n) \subseteq m$, což je spor s $m \subset \mathcal{S}(n)$. □

Lemma 5.46. *Relace $\in$ je lineární ostré uspořádání na ω. Neboli pro všechna $k, n, m \in \omega$ platí*

(i) $n \notin n$, *… antireflexibilita*

(ii) $m \in n \wedge n \in k \Rightarrow m \in k$, *… tranzitivita*

(iii) $m \in n \vee m = n \vee n \in m$. *… trichotomie*

Důkaz. (i) Jak jsme dokázali v Lemma 5.43.

(ii) Podle předchozího lemma lze relaci $\in$ zaměnit za $\subset$, což je tranzitivní.

(iii) Pro pevně zvolené n to dokážeme indukcí podle m. Definujme množinu

$$X(n) \coloneqq \{m \in \omega \mid m \in n \vee m = n \vee n \in m\}.$$

Dokážeme, že $X(n)$ je induktivní a tedy $X(n) = \omega$. Nejprve uvažme $n = 0$. Určitě $0 \in X(0)$, protože $0 = 0$. Indukční krok: je-li $m \in X(0)$, tak buď $m = 0$ nebo $0 \in m$. Každopádně $0 \in m \cup \{m\} = \mathcal{S}(m)$ a tedy $\mathcal{S}(m) \in X(0)$. Z toho také vyplývá, že pro každé $n \in \omega$ je $0 \in X(n)$. Nyní zvolme $n \neq 0$ a $m \in X(n)$.

(a) Pokud $m \in n$, tak podle předchozího lemma $m \subset n$. Také $\{m\} \subseteq n$, tedy $\mathcal{S}(m) \subseteq n$. Pokud $\mathcal{S}(m) = n$ tak jsme hotoví. Pokud $\mathcal{S}(m) \subset n$, tak podle předchozího lemma $\mathcal{S}(m) \in n$.

(b) Jinak $m = n$ nebo $n \in m$, každopádně $n \in m \cup \{m\} = \mathcal{S}(m)$.

V obou případech $\mathcal{S}(m) \in X(n)$, tudíž $X(n) = \omega$. □

Věta 5.47. *ω je dobře ostře uspořádaná relací $\in$.*

Důkaz. Nechť $\varnothing \neq a \subseteq \omega$. Jelikož $\in$ je lineární na ω, tak nám stačí najít minimální prvek a (bude automaticky i nejmenší). Zvolme nějaké $n \in a$. Pokud je minimální, tak jsme vyhráli. Jinak nechť $b \coloneqq n \cap a$. Protože n je konečná, tak b je konečná (a neprázdná). Podle Lemma 5.25 má b minimální prvek, označme jej m. Tvrdíme, že m je minimální i v a. Kdyby existovalo nějaké $x \in a$ takové, že $x \in m$ (je menší než m), tak dojdeme ke sporu. Jelikož $x \in m \in n$, tak $x \in n$ a máme $x \in b$. Ale m je minimální v b. □

Úmluva 5.48. Od teď budeme dobře (ostře) uspořádanou množinu $(\omega, \in)$ psát jako $(\omega, <)$ a pro přirozená čísla budeme psát $n < m$ namísto $n \in m$.

Další věta nám umožní poznat, kdy je něco uspořádané stejně jako ω.

Věta 5.49 (O charakterizaci uspořádání ω)**.** *Nechť $(A, <_R)$ je lineárně uspořádaná nekonečná množina splňující pro každé $a \in A$, že $(\leftarrow, a]$ je konečná. Potom je '$<_R$' dobré uspořádání a navíc jsou uspořádané množiny $(A, <_R)$ a $(\omega, <)$ izomorfní.*

Důkaz. První část je téměř stejná jako důkaz poslední věty. Nechť $\varnothing \neq c \subseteq A$ a $a \in c$. Pokud a není minimální (nejmenší), tak označme $b \coloneqq c \cap (\leftarrow, a]$. Platí $a \in b$, takže $\varnothing \neq b \subseteq (\leftarrow, a]$. Podle předpokladu je b konečná, takže má minimální prvek m. Chceme ukázat, že m je minimální i v c. Pro spor nechť existuje nějaké $x \in c$ takové, že $x <_R m$. Ukážeme, že $x \in b$, což bude spor. Protože $x <_R m <_R a$, tak $x \in (\leftarrow, a]$ a navíc $x \in c$, takže $x \in b$.

Zbývá ukázat, že $(A, <_R)$ a $(\omega, <)$ jsou izomorfní. Podle Věty 4.47 nastane jedna ze dvou možností:

(a) A je izomorfní s nějakou dolní podmnožinou $B \subseteq \omega$. Tvrdíme, že B není shora omezená. Kdyby byla, tak by existovalo nějaké $n \in \omega$ takové, že $b < n$ pro všechny $b \in B$. Čili $B \subseteq n$, jelikož $b < n$ znamená $b \in n$, takže B by byla konečná, což je spor s $A \approx B$, protože A je nekonečná. Jelikož B není shora omezená, tak každé $n \in \omega$ je menší než nějaký prvek B a tedy $n \in B$, protože B je dolní podmnožina. Tudíž $B = \omega$.

(b) ω je izomorfní s nějakou dolní podmnožinou $C \subseteq A$. Opět C není omezená, stejným argumentem. A opět $C = A$, protože C je dolní podmnožina. □

5.5 Spočetné a nespočetné množiny

Klasifikujeme množiny podle jejich vztahu k přirozeným číslům. Připomeňme, že množina x je konečná, pokud $x \approx n$ pro nějaké $n \in \omega$.

Definice 5.50 (Spočetnost)**.** Množina x je

- *spočetná*, pokud $x \approx \omega$,
- *nejvýše spočetná*, pokud je spočetná nebo konečná,
- *nespočetná*, pokud není nejvýše spočetná.

Poznámka. Pojmem „spočetná množina“ se často myslí „nejvýše spočetná.“ Pokud to chceme rozlišit, tak můžeme použít termín „spočetně nekonečná.“ Ale v tomto textu budeme používat terminologii zavedenou výše.

Tvrzení 5.51. *Pro množinu všech přirozených čísel platí, že*

(i) *každá shora omezená podmnožina $A \subseteq \omega$ je konečná,*

(ii) *každá shora neomezená podmnožina $A \subseteq \omega$ je spočetná.*

Důkaz.

(i) Pokud je A shora omezená číslem $n \in \omega$, pak $A \subseteq \mathcal{S}(n)$, tedy A je konečná.

(ii) Je-li $A \subseteq \omega$ konečná, tak má podle Lemma 5.25 maximální (největší) prvek, tedy je omezená. Obměnou: je-li A neomezená, pak je nekonečná. Potřebujeme ale spočetnost. Jelikož je A nekonečná, lineárně uspořádaná relací $<$ a pro každé n je $(\leftarrow, n] \subseteq \mathcal{S}(n)$ konečná, tak uspořádané množiny $(A, <)$ a $(\omega, <)$ jsou izomorfní podle Věty 5.49. Speciálně $A \approx \omega$. □

Důsledek 5.52. *Množina x je nejvýše spočetná $\iff$ $x \preceq \omega$.*

Důsledek 5.53. *Každá podmnožina spočetné množiny je nejvýše spočetná.*

Důkaz. Nechť je A spočetná, $f : A \to \omega$ bijekce, a $B \subseteq A$ podmnožina. Potom $B \approx f[B] \subseteq \omega$, tedy $B \preceq \omega$. □

5.5.1 Operace zachovávající spočetnost

Definice 5.54. Definujeme *lexikografické* (ostré) uspořádání $<_L$ na $\omega \times \omega$ jako

$$(m_1, n_1) <_L (m_2, n_2) \iff \begin{cases} m_1 < m_2, \text{ nebo} \\ m_1 = m_2 \wedge n_1 < n_2. \end{cases}$$

Intuice. Lexikografické uspořádání je dobré na $\omega \times \omega$. Prvky jsou vlastně uspořádané do mřížky, sloupečky jsou nekonečné stoupající řetězce a n-tý sloupeček je menší než $(n+1)$-ní sloupeček.

Příklad. Platí, že $(\omega \times 2, <_L)$, tedy nekonečně sloupečků výšky dva, je izomorfní s $(\omega, <)$. Ale $(2 \times \omega, <_L)$, tedy dva nekonečné sloupečky, není izomorfní s $(\omega, <)$, přestože je dobře uspořádaná. Tohle lze snadno ověřit pomocí Věty 5.49.

Definice 5.55. Definujeme *maximo-lexikografické* (ostré) uspořádání $\sqsubset$ na $\omega \times \omega$ jako

$$(m_1, n_1) \sqsubset (m_2, n_2) \iff \begin{cases} \max\{m_1, n_1\} < \max\{m_2, n_2\}, \text{ nebo} \\ \max\{m_1, n_1\} = \max\{m_2, n_2\} \wedge (m_1, n_1) <_L (m_2, n_2). \end{cases}$$

Intuice. Procházíme jakoby čtverce nebo pravé úhly v nějaké vzdálenosti od počátku, a věci ve stejné vzdálenosti procházíme lexikograficky. Tohle je možná dobré si namalovat na kus papíru.

Úloha 5.56. Ověřte pomocí Věty 5.49, že $(\omega \times \omega, \sqsubset)$ je izomorfní s $(\omega, <)$.

Důsledek 5.57. $\omega \times \omega \approx \omega$.

Poznámka. Tohle jsme dokázali již dříve pomocí základní věty aritmetiky, ale teď to umíme i bez ní. Přístup s uspořádáním $\sqsubset$ je navíc mnohem obecnější, protože v jeho definici můžeme nahradit ω za jakoukoliv jinou dobře uspořádanou množinu $(w, <)$. Pak lze ukázat (ale my na to zatím nemáme nástroje), že uspořádané množiny $(w \times w, \sqsubset)$ a $(w, <)$ jsou izomorfní, a tudíž $w \times w \approx w$.

Důsledek 5.58. *Množiny $\mathbb{Z}$ a $\mathbb{Q}$ jsou spočetné. V sekci 5.2 jsme to dokázali pomocí aritmetiky, ovšem teď to umíme i bez ní.*

Ukážeme, že podobně jako konečné sjednocení nebo konečný součin konečných množin je konečný, vyrobit ze spočetných množin nespočetnou množinu není jen tak.

Věta 5.59. *Jsou-li A, B spočetné množiny, pak $A \cup B$ a $A \times B$ jsou také spočetné.*

Důkaz. Nechť $f : A \to \omega$ a $g : B \to \omega$ jsou bijekce. Definujeme zobrazení $h : A \cup B \to \omega \times 2$ jako

$$h(x) := \begin{cases} (f(x), 0), & \text{pro } x \in A, \\ (g(x), 1), & \text{jinak.} \end{cases}$$

Zobrazení h je prosté, takže $A \cup B \preceq \omega \times 2 \approx \omega$. Navíc $\omega \approx A \subseteq A \cup B$, takže $\omega \preceq A \cup B$. Podle Cantor–Bernsteinovy věty platí $A \cup B \approx \omega$.

Nyní pro $A \times B$. Definujeme $j : A \times B \to \omega \times \omega$ jako $j : (a, b) \mapsto (f(a), g(b))$. Všimněme si, že j je bijekce, tedy $A \times B \approx \omega \times \omega \approx \omega$. □

Důsledek 5.60. *Konečná sjednocení a konečné kartézské součiny spočetných množin jsou spočetné.*

Důkaz. Indukcí; můžeme použít jak princip indukce pro konečné množiny, tak princip indukce pro přirozená čísla (díky Větě 5.42). □

Důsledek 5.61 (Dirichletův princip pro nespočetné množiny). *Je-li nespočetná množina sjednocením konečně mnoha množin, tak alespoň jedna z nich je nespočetná.*

Věta 5.62. *Je-li A spočetná množina, potom*

(a) *množina $[A]^{<\omega}$ všech konečných podmnožin množiny A je spočetná,*

(b) *množina $A^{<\omega}$ všech konečných posloupností prvků množiny A je spočetná.*

Důkaz. Jelikož A je spočetná, tak můžeme předpokládat, že $A = \omega$. Mohli bychom definovat nějaké vhodné uspořádání na $[\omega]^{<\omega}$ a ověřit že splňuje podmínky Věty 5.49, a z toho $[\omega]^{<\omega} \approx \omega$. Potom si můžeme uvědomit že konečné posloupnosti přirozených čísel jsou vlastně prvky $[\omega \times \omega]^{<\omega}$, a jelikož $\omega \times \omega = \omega$, tak $\omega^{<\omega} \approx \omega$.

Tento přístup je popsaný v Příkladu 6.28 v první kapitole Balcar–Štěpánka [1], ale jednodušší (přestože koncepčně méně čisté) je kódování pomocí prvočísel. Zjevně $\omega \preceq [\omega]^{<\omega} \preceq \omega^{<\omega}$. Definujeme prosté zobrazení $f : \omega^{<\omega} \to \omega$. Jelikož prvočísel je nekonečně mnoho, existuje bijektivní zobrazení π které je enumeruje; tedy $\pi(n)$

je n-té nejmenší prvočíslo, kde indexujeme od nuly. Konečnou posloupnost $\bar{x} = (x_0, x_1, \ldots, x_{n-1}) \in \omega^{<\omega}$ pak můžeme zakódovat jako součin

$$f(\bar{x}) \coloneqq \prod_{i<n} \pi(i)^{x_i}.$$

Toto zobrazení je prosté ze základní věty aritmetiky. $\square$

Poznámka. Obecněji se pomocí axiomu výběru dá dokázat, že $[A]^{<\omega} \approx A^{<\omega} \approx A$ pro jakoukoliv nekonečnou množinu A.

Zdá se, že na to, abychom ze spočetné množiny vyrobili nespočetnou, bude potřeba nějaká nekonečná operace. Co kdybychom udělali sjednocení nebo součin spočetně mnoha spočetných množin? Tyto pojmy si formálně definujeme až v kapitole o axiomu výběru, zatím je můžeme vnímat intuitivně. Ukážeme, že součin bude nespočetný, nehledě na platnost axiomu výběru. Spočetnost sjednocení nelze v ZF rozhodnout, ale ukážeme, že v ZFC bude sjednocení spočetné.

5.5.2 Cantorova věta

Věta 5.63 (Cantor)**.** *Pro každou množinu x platí $x \prec \mathcal{P}(x)$.*

Cantor tuto větu dokázal svojí slavnou diagonalizační metodou. Než ji dokážeme, tak tuto metodu demonstrujeme na případu $\omega \prec \mathcal{P}(\omega)$.

Tvrzení 5.64. *$\omega \prec \mathcal{P}(\omega)$.*

Důkaz. Zjevně $\omega \preceq \mathcal{P}(\omega)$, pomocí prostého zobrazení $\omega \to \mathcal{P}(\omega)$ definovaného jako $n \mapsto \{n\}$. Navíc si vzpomeňme, že jsme v Lemma 5.4 pomocí charakteristických funkcí podmnožin $A \subseteq \omega$ ukázali, že $\mathcal{P}(\omega) \approx {}^{\omega}2$. Pro spor tedy můžeme předpokládat, že existuje bijekce $f : \omega \to {}^{\omega}2$, která každé nekonečné posloupnosti nul a jedniček přiřadí jednoznačné přirozené číslo.

Označme jako $\pi_n \coloneqq f(n)$ posloupnost, která dostala číslo n. Ukážeme, že nějaká posloupnost $\sigma : \omega \to 2$ musí chybět (nedostala žádné číslo). Její n-tý člen $\sigma(n)$ definujeme jako $1 - \pi_n(n)$. Tedy pokud π_n měla na n-té pozici jedničku, tak jsme do σ napsali nulu, a naopak. Jelikož se σ liší od každé z posloupností π_n, konkrétně na n-té pozici, tak jí nemohlo být přiřazeno žádné číslo, a f tudíž není bijekce. Spor. $\square$

Důsledek 5.65. *Množina $\mathcal{P}(\omega)$ je nespočetná.*

Nyní dokážeme Cantorovu větu. Přestože se důkaz může zdát jiný než důkaz předchozího tvrzení, všimněme si, že využívá naprosto stejnou myšlenku.

Důkaz Věty 5.63. Zjevně $x \preceq \mathcal{P}(x)$, pomocí prostého zobrazení $x \to \mathcal{P}(x)$ definovaného jako $a \mapsto \{a\}$. Pro spor předpokládejme, že existuje bijekce $f : x \to \mathcal{P}(x)$. Definujme množinu $T \coloneqq \{a \in x \mid a \notin f(a)\}$. Nyní pro každé $a \in x$ nastane jedna ze dvou situací:

$$\begin{aligned} a \in T &\implies a \notin f(a) \implies T \neq f(a), \\ a \notin T &\implies a \in f(a) \implies T \neq f(a). \end{aligned}$$

V každém případě $T \neq f(a)$, takže T nemá vzor, což je spor s tím, že f je bijekce. $\square$

Důsledek 5.66. *Univerzální třída* $\mathbf{V}$ *je vlastní třídou.*

Důkaz. Kdyby byla množinou, tak $\mathbf{V} \prec \mathcal{P}(\mathbf{V})$. Ale určitě $\mathcal{P}(\mathbf{V}) \preceq \mathbf{V}$, což je spor. $\square$

Důsledek 5.67. *Pro každé $n \geq 1$ je třída všech n-prvkových množin vlastní třídou.*

Důkaz. Kdyby byla množinou, tak z axiomu sumy by byla její suma také množina. Ale její suma je $\mathbf{V}$. □

Úloha 5.68. Řekneme, že funkce $f : \omega \to \omega$ *nakonec dominuje* funkci $g : \omega \to \omega$, pokud existuje nějaké $n_0 \in \omega$ takové, že pro všechna $n \geq n_0$ platí $f(n) > g(n)$. Dokažte diagonalizační metodou, že pro každou rodinu funkcí $\{g_n : \omega \to \omega \mid n \in \omega\}$ existuje nějaká funkce $f : \omega \to \omega$, která je všechny nakonec dominuje.

5.5.3 Kardinalita kontinua

Kardinalitou *kontinua* myslíme mohutnost množiny reálných čísel. Tento název se ujal, protože standardní uspořádání reálných čísel je úplné (nemá žádné „díry“).

Dedekindovy řezy Než začneme něco dokazovat, tak předvedeme jednu z možných konstrukcí reálných čísel, konkrétně pomocí takzvaných *dedekindových řezů.*

Definice 5.69. Množina $X \subseteq \mathbb{Q}$ je *dedekindův řez*, pokud

(i) X je dolní podmnožina $\mathbb{Q}$,

(ii) existuje-li $\sup_{\mathbb{Q}}(X)$, potom $\sup_{\mathbb{Q}}(X) \in X$.

Takže třeba $\mathbb{Q} \cap (-\infty, 1)$ není dedekindův řez, ale $\mathbb{Q} \cap (-\infty, 1]$ ano. Jinak by to nebylo jednoznačné. Ovšem $\mathbb{Q} \cap (-\infty, \sqrt{2}) = \mathbb{Q} \cap (-\infty, \sqrt{2}]$ je dedekindův řez, protože tato množina nemá v $\mathbb{Q}$ supremum.

Reálná čísla pak můžeme definovat jako množinu všech dedekindových řezů $X \subseteq \mathbb{Q}$ uspořádaných inkluzí.

S reálnými čísly však většinou pracujeme jako s nekonečnými nápisy v desítkové soustavě, obsahujícími konečný prefix následovaný tečkou a nekonečným sufixem desetinných míst. Pro nás bude praktičtější je interpretovat ve dvojkové soustavě.

Věta 5.70. ${}^{\omega}2 \approx \mathcal{P}(\omega) \approx \mathbb{R} \approx [0, 1]$.

Důkaz. $\mathcal{P}(\omega) \approx {}^{\omega}2$ už víme z Lemma 5.4. Jako další ukážeme $[0, 1] \approx {}^{\omega}2$.

(i) $[0, 1] \preceq {}^{\omega}2$. Číslo $a \in [0, 1]$ zapíšeme binárně. Pokud $a = 0$, tak máme $0.000\ldots$ a pokud $a > 0$, tak $0.a_0a_1a_2\ldots$, kde nekonečně mnoho a_i je 1 abychom odstranili duplicity pro periodická čísla. Takže třeba $0.5_{10} = 0.1_2$ zapíšeme jako $0.0111\ldots$. Tyto nekonečné posloupnosti jsou zjevně funkce z ω do $\{0, 1\}$.

(ii) ${}^{\omega}2 \preceq [0, 1]$. Problém je, že posloupnosti $0.1000\ldots$ a $0.0111\ldots$ se zobrazí na stejné reálné číslo. Ale kdybychom to četli ve trojkové soustavě, tak už to budou různá čísla. Proto definujeme funkci $f : {}^{\omega}2 \to [0, 1]$ jako

$$(a_0, a_1, a_2, \ldots) \mapsto \sum_{i=0}^{\infty} \frac{a_i}{3^{i+1}}.$$

Podle Cantor–Bernsteinovy věty platí $\mathcal{P}(\omega) \approx {}^{\omega}2 \approx [0, 1]$. Zbývá ukázat $[0, 1] \approx \mathbb{R}$. Zřejmě $[0, 1] \preceq \mathbb{R}$, protože $[0, 1] \subseteq \mathbb{R}$. Opačně $\mathbb{R} \preceq [0, 1]$ například prostou funkcí

$$\arctan : \mathbb{R} \to (-\pi/2, \pi/2),$$

kterou vhodně upravíme, aby obor hodnot byl podmnožinou intervalu $[0, 1]$. □

Úloha 5.71. Ukažte, že $[0,1]^2 \approx [0,1]$, tedy čtverec se zobrazí na úsečku. Jelikož $[0, 1] \approx \mathbb{R}$, tak dostáváme $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$, tedy plocha se zobrazí na přímku.

Řešení. Pokud si nevíte rady, tak hezky vysvětlené řešení je v [2].

5.5.4 Hypotéza kontinua

Ukázali jsme, že reálných čísel je více než přirozených. Je přirozené položit si otázku, zda existuje něco mezi? Bylo by hezké, kdyby nejmenší množina, větší než přirozená čísla, byla reálná přímka (kontinuum). Tato myšlenka se nazývá hypotéza kontinua, anglicky Continuum Hypothesis (CH). Formuloval ji už Cantor a říká, že neexistuje žádná množina x taková, že

$$\omega \prec x \prec \mathcal{P}(\omega) \approx \mathbb{R}.$$

Tedy každá nekonečná $x \subseteq \mathbb{R}$ je buď spočetná, nebo ekvivalentní s $\mathbb{R}$. Gödel (1940) dokázal, že CH nelze v ZFC vyvrátit. Cohen (1963) dokázal, že nelze v ZFC dokázat. Tedy je možné k ZFC bezesporně přidat jako axiom CH i $\neg\mathsf{CH}$.

5.5.5 Algebraická čísla

Definice 5.72. *Algebraická čísla* jsou reálné kořeny polynomů s celočíselnými koeficienty. Reálná čísla, která nejsou algebraická, nazýváme *transcendentní.*

Takže například $\sqrt{2}$ je algebraické číslo, protože je kořenem polynomu $x^2 - 2$.

Tvrzení 5.73. *Algebraických čísel je spočetně mnoho.*

Důkaz. Polynom s celočíselnými koeficienty můžeme reprezentovat jako konečnou posloupnost $(a_0, a_1, \ldots, a_n)$ celých čísel. Celých čísel je spočetně mnoho, takže těchto posloupností je podle Věty 5.62 také pouze spočetně mnoho.

Tedy každému polynomu s celočíselnými koeficienty můžeme přiřadit nějaké unikátní pořadové číslo $k \in \omega$. Navíc víme, že polynom stupně n má nejvýše n různých reálných kořenů. Algebraických čísel je určitě alespoň spočetně mnoho, musíme ukázat, že jich není víc. Proto definujeme prosté zobrazení všech algebraických čísel do spočetné množiny $\omega \times \omega$. Každý reálný kořen x polynomu

$$a_0 + a_1x^1 + \cdots + a_{n-1}x^{n-1} + a_nx^n = 0, \qquad a_n \neq 0$$

je jednoznačně určen dvojicí (k, ℓ), kde k je číslo přiřazené tomuto polynomu a ℓ udává, že x je ℓ-tý nejmenší[5] reálný kořen tohoto polynomu. Ovšem jedno algebraickém číslo může být kořenem více různých polynom — rovnici stačí vynásobit nějakou konstantou. Proto algebraickému číslu x přiřadíme ze všech dvojic (k, ℓ), které mu odpovídají, tu, kde je k nejmenší možné. $\square$

Z Dirichletova principu pro nespočetné množiny pak dostáváme nejenom to, že transcendentní čísla existují (přestože jsme žádné nesestrojili!), ale dokonce, že *skoro všechna* reálná čísla jsou transcendentní:

Důsledek 5.74. *Transcendentních čísel je nespočetně mnoho.*

[5] Neuvažujeme opakované kořeny.

6 Axiom výběru

Axiom výběru, anglicky Axiom of Choice (AC), už jsme zmínili mnohokrát. Jeho přidáním do ZF získáme teorii ZFC. Připomeňme, že pokud je ZF konzistentní,[6] potom je ZFC také konzistentní. Čili to, zda věříme nebo nevěříme axiomu výběru, je čistě filozofické rozhodnutí, na konzistenci teorie množin to nic nezmění.

Bez axiomu výběru nelze dokázat mnoho věcí, které by intuitivně měly platit, ale zároveň byl historicky kontroverzní, protože některé jeho důsledky jsou na hranici paradoxnosti. Například princip dobrého uspořádání, který říká, že každou množinu lze dobře uspořádat.[7] Dále pomocí axiomu výběru lze zkonstruovat podmnožiny reálných čísel, které nejsou Lebesgueovsky měřitelné, což je jádro slavného Banach–Tarskiho paradoxu. Ten uvádí postup, jak rozdělit jednotkovou kouli na konečný počet částí a tyto části přeskupit tak, aby vznikly dvě koule identické s tou původní.

Axiom výběru je také velmi důležitý mimo teorii množin, kde jeho slabší varianty, jako jsou axiom spočetného nebo axiom závislého výběru, využíváme implicitně a ani si to neuvědomujeme. Tyto dvě zmíněné slabší varianty ovšem naštěstí neumožňují zrekonstruovat paradoxy zmíněné výše.

6.1 Indexované soubory množin

Definice 6.1. *Indexovaný soubor množin* $\langle X_i \mid i \in I \rangle$ je zobrazení F s definičním oborem I, kde X_i označuje množinu $F(i)$. Říkáme, že I je *indexová třída* tohoto souboru a že x *patří do souboru*, jestliže pro nějaké $i \in I$ platí $x = X_i$. Definujeme

$$\bigcup_{i\in I} X_i \coloneqq \bigcup \mathrm{Rng}(F),$$
$$\bigcap_{i\in I} X_i \coloneqq \bigcap \mathrm{Rng}(F),$$
$$\bigtimes_{i\in I} X_i \coloneqq \Big\{ f \mid f : I \to \bigcup_{i\in I} X_i \ \wedge\ (\forall i \in I)(f(i) \in X_i) \Big\}.$$

Definice kartézského součinu má smysl jen pro soubory indexované množinou, protože vlastní třídy nebohou nikam náležet.

Lemma 6.2. *Je-li indexová třída I souboru $\langle X_i \mid i \in I \rangle$ množinou, potom jsou třídy $\bigcup_{i\in I} X_i$, $\bigcap_{i\in I} X_i$ a $\bigtimes_{i\in I} X_i$ také množinami.*

Důkaz. $\mathrm{Dom}(F) = I$ je množina, takže z axiomu nahrazení je $\mathrm{Rng}(F) = F[I]$ také množina. Proto jsou suma a průnik také množiny. Kartézský součin je podmnožinou třídy všech zobrazení z I do $\bigcup_{i\in I} X_i$, což je podle Lemma 4.31 množina. □

Pozorování 6.3. *Pokud pro každé $i \in I$ je $X_i = X$, tak $\bigtimes_{i\in I} X_i = {}^I X$.*

Lemma 6.4. *Je-li $\langle X_i \mid i \in \omega \rangle$ soubor spočetně mnoha množin splňujících $2 \preceq X_i$, kde na každém X_i navíc existuje dobré uspořádání, potom je kartézský součin tohoto souboru nespočetný.*

Důkaz. Není těžké ukázat, že
$$\bigtimes_{i\in\omega} 2 \preceq \bigtimes_{i\in\omega} X_i,$$

[6] Tedy má model, nebo ekvivalentně, není v ní možné dokázat spor.

[7] Speciálně reálná čísla lze dobře uspořádat. Tedy že z každé neprázdné podmnožiny reálných čísel lze vybrat nějaké kanonické nejmenší číslo. Co je například nejmenší číslo v intervalu $(0, 1)$?

prostě z každého X_i nejprve vezmu nejmenší prvek, a potom druhý nejmenší. Podle předchozího pozorování ovšem platí $\bigtimes_{i \in \omega} 2 = {}^{\omega}2 \approx \mathcal{P}(\omega)$, což je podle Cantorovy věty nespočetná množina. $\square$

Důsledek 6.5. *Kartézský součin spočetně mnoha spočetných množin je nespočetný.*

6.2 Co axiom výběru tvrdí

V této sekci motivujeme a zavedeme axiom výběru. Mějme f, zobrazení množiny X na množinu Y a podívejme se na rozklad množiny X definovaný jako

$$r \coloneqq \{f^{-1}[y] \mid y \in Y\}.$$

Existuje prosté zobrazení $g : Y \to X$?

- Pro konečné Y lze dokázat principem indukce pro konečné množiny. Neformálně si prostě konečně-mnohokrát vezmu nějaký prvek z $f^{-1}[y]$, jednou pro každé y.
- Pro dobře uspořádané X vezmu z $f^{-1}[y]$ vždy ten nejmenší prvek.
- Obecně to v ZF dokázat nelze — museli bychom pro každé $y \in Y$ *vybrat* nějakého reprezentanta $x \in f^{-1}[y]$, ale pokud $f^{-1}[y]$ není dobře uspořádané, není jasné, jak to udělat. I když $f^{-1}[y]$ třeba lze dobře uspořádat, musíme opět *vybrat* nějaké dobré uspořádání, které použijeme.

Tento problém motivuje následující formulaci axiomu výběru:

Axiom 6.6 (Princip výběru)**.** Pro každou množinu X a každý její rozklad r existuje *výběrová množina* $v \subseteq X$ taková, že pro každou rozkladovou třídu $u \in r$ obsahuje v jednoho jediného reprezentanta $x \in u$. Tedy $u \cap v = \{x\}$.

Jiná, šikovnější formulace používá takzvané *výběrové funkce* neboli *selektory*.

Definice 6.7. *Selektor* na množině x je funkce $f : x \to \bigcup x$ splňující

$$(\forall t \in x)(t \neq \varnothing \Rightarrow f(t) \in t).$$

Ekvivalentně můžeme předpokládat, že selektor je definovaný pouze na množině $x \setminus \{\varnothing\}$ a pro každé $t \in \mathrm{Dom}(f)$ platí $f(t) \in t$.

Axiom 6.8 (Axiom výběru AC)**.** Na každé množině existuje selektor.

Ukážeme, že axiom výběru a princip výběru jsou skutečně ekvivalentní.

Tvrzení 6.9. *Následující tvrzení jsou ekvivalentní.*

(1) *Axiom výběru.*

(2) *Princip výběru.*

(3) *Pro každou relaci S, která je množinou, existuje funkce $f \subseteq S$ taková, že* $\mathrm{Dom}(f) = \mathrm{Dom}(S)$.

(4) *Kartézský součin neprázdného souboru neprázdných množin je neprázdný.*

Důkaz. (1)⇒(2) Nechť r je rozklad X, podle axiomu výběru existuje selektor f na r. Hledaná výběrová množina je $\mathrm{Rng}(f)$.

(2)⇒(3) Pokud $S = \varnothing$, potom $f = \varnothing$ a není co dokazovat. Proto nechť $S \neq \varnothing$. Definujeme rozklad r množiny S jako

$$r \coloneqq \big\{\{(x,y) \in S \mid y \in \mathrm{Rng}(S)\} \,\big|\, x \in \mathrm{Dom}(S)\big\}.$$

Podle principu výběru existuje výběrová množina tohoto rozkladu, což je právě hledaná funkce f.

(3)⇒(4) Neprázdný soubor neprázdných množin $\langle X_i \mid i \in I \rangle$ určuje relaci[8]

$$S \coloneqq \{(i,x) \mid i \in I \wedge x \in X_i\}.$$

Podle (3) existuje funkce $f \subseteq S$ taková, že $\mathrm{Dom}(f) = \mathrm{Dom}(S) = I$ a tedy f je prvkem uvažovaného produktu.

(4)⇒(1) Nechť x je libovolná množina, BÚNO $x \neq \varnothing$ a $\varnothing \notin x$. Tedy x určuje neprázdný soubor neprázdných množin $\langle y \mid y \in x \rangle$, který má podle (4) neprázdný kartézský součin. Všimněme si, že každý prvek tohoto součinu je selektorem na x. □

6.3 Přehled důsledků axiomu výběru

Uvedeme některé ekvivalentní formulace a důsledky axiomu výběru. Více detailů a důkazy většiny z nich lze nalézt v [3].

Axiom výběru AC

$\iff$ Pro každou nekonečnou množinu x platí, že $x \times x \approx x$.

$\iff$ Každý vektorový prostor (i nekonečné dimenze) má bázi.

$\iff$ Každý produkt (i nekonečný) kompaktních topologických prostorů je kompaktní.

$\iff$ Každý souvislý (i nekonečný) graf má kostru.

$\implies$ Věta o kompaktnosti pro logiku prvního řádu: pokud každá konečná podteorie teorie T má model, pak celá teorie T má také model.

$\implies$ Existuje zobrazení co každé množině x přiřadí množinu $|x|$ takovou, že $x \approx |x|$, a navíc pro každé dvě množiny x a y splňuje $x \approx y \iff |x| = |y|$.

$\iff$ **Zornovo lemma**, také známé jako **princip maximality:** pokud neprázdná uspořádaná množina $(A, \leq)$ splňuje, že každý řetězec je shora omezený, pak A obsahuje maximální prvek.

$\iff$ **Princip trichotomie:** relace $\preceq$ je trichotomická, neboli pro každé dvě množiny x a y platí buď $x \preceq y$ nebo $y \preceq x$.

$\iff$ **Princip dobrého uspořádání:** každou množinu lze dobře uspořádat.

Posledním třem[9] se budeme věnovat trochu podrobněji a dokážeme některé implikace mezi nimi a axiomem výběru. Celý důkaz jejich ekvivalence se nachází ve skriptíčkách k následujícímu předmětu [6].

[8] Proč je S množina?

[9] "The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?" — Jerry Bona

6.4 Axiom spočetného výběru

Axiom 6.10 (Axiom spočetného výběru AC_ω)**.** Na každé spočetné množině existuje selektor. Tedy můžeme udělat pouze spočetně mnoho výběrů.

Následující ještě slabší varianta stále nelze v ZF dokázat.

Axiom 6.11 (Axiom spočetného výběru pro konečné množiny $\mathsf{AC}_\omega^{\mathsf{fin}}$)**.** Na každé spočetné množině konečných množin existuje selektor. Tedy můžeme udělat pouze spočetně mnoho výběrů, a navíc pouze z konečných množin.

Tyto slabší axiomy nemají žádné paradoxické důsledky typu Banach–Tarskiho paradox, ale za to mají spoustu hezkých a užitečných důsledků.

Axiom spočetného výběru pro konečné množiny $\mathsf{AC}_\omega^{\mathsf{fin}}$

$\iff$ Sjednocení spočetně mnoha konečných množin je nejvýše spočetné.

$\iff$ Königovo lemma: každý nekonečný zakořeněný strom, jehož každý vrchol má konečný stupeň, obsahuje nekonečnou větev (cestu pryč od kořene).

Axiom spočetného výběru AC_ω

$\implies$ Sjednocení spočetně mnoha spočetných množin je spočetné.

$\implies$ Každá nekonečná množina x má spočetnou podmnožinu; neboli $\omega \preceq x$.

$\implies$ Množina x je konečná $\iff$ je dedekindovsky konečná.

$\implies$ Reálná funkce $f : \mathbb{R} \to \mathbb{R}$ je spojitá $\iff$ pro každou konvergentní posloupnost reálných čísel $(x_n)_{n\in\omega}$ platí $\lim f(x_n) = f(\lim x_n)$.

Některé z těchto důsledků teď dokážeme.

Tvrzení 6.12 (AC_ω)**.** *Sjednocení spočetně mnoha spočetných množin je spočetné.*

Důkaz. Uvažme soubor $\langle X_n \mid n \in \omega \rangle$ spočetně mnoha spočetných množin $X_n \approx \omega$. Sestrojíme prosté zobrazení $S := \bigcup_{n\in\omega} X_n$ do spočetné množiny $\omega \times \omega$. Pro každé $n \in \omega$ *vybereme* nějaké prosté zobrazení $j_n : X_n \to \omega$ (všimněme si, že děláme pouze spočetně mnoho výběrů). Formálně uvážíme množinu $A := \{E_n \mid n \in \omega\}$, kde E_n je (neprázdná) množina všech prostých zobrazení $j : X_n \to \omega$. Podle AC_ω existuje selektor f na A a položíme $j_n := f(E_n)$.

Pro prvek $x \in S$ definujeme

$$n_x := \min\{n \in \omega \mid x \in X_n\}.$$

Toto číslo nám říká, v jaké množině X_n se x objeví poprvé. Všimněme si, že přestože více různých $x \in S$ může mít stejné číslo n_x, tak zobrazení $g : x \mapsto (n_x, j_{n_x}(x))$ je prosté, jelikož j_n jsou prostá. $\square$

Fakt 6.13. *V* ZF *je bezesporné předpokládat, že nespočetná množina* $\mathbb{R}$ *je sjednocením spočetně mnoha spočetných množin.*

Dále se budeme zabývat Dedekindovou definicí konečnosti. Připomeňme, že každá konečná množina je i dedekindovsky konečná, a tedy (obměnou) každá dedekindovsky nekonečná množina je nekonečná.

Fakt 6.14. *V* ZF *mohou existovat nekonečné, ale dedekindovsky konečné množiny.*

Pozorování 6.15. *Je-li množina x nekonečná, ale dedekindovsky konečná, pak neobsahuje žádnou spočetnou podmnožinu $y \subseteq x$; neboli $\omega \npreceq x$.*

Důkaz. Předpokládejme, že x obsahuje spočetnou podmnožinu $y = \{a_0, a_1, a_2, \dots\}$. Potom můžeme sestrojit bijekci $g : x \to x \setminus \{a_0\}$ předpisem $g(a) = a$, pokud $a \notin y$, a $g(a_n) = a_{n+1}$ pro každé $n \in \omega$. □

Takové množiny x jsou tedy nespočetné, avšak neplatí, že $\omega \prec x$.

Věta 6.16 (AC_ω)**.** *Každá nekonečná množina obsahuje spočetnou podmnožinu. Každá nekonečná množina je tedy dedekindovsky nekonečná a každá dedekindovsky konečná množina je konečná.*

Důkaz. Nechť x je nekonečná množina. Protože pro každé $n \in \omega$ platí $n \prec x$, můžeme pomocí AC_ω pro každé $n \in \omega$ *vybrat* prosté zobrazení $G_n : n \to x$. Každé zobrazení G_n odpovídá nějaké posloupnosti $a_0, a_1, \dots, a_{n-1}$. Zapíšeme-li prvky všech posloupností $G_0, G_1, G_2, \dots, G_n, \dots$ za sebe a následně z výsledné posloupnosti odstraníme všechny výskyty každého prvku $a \in x$ kromě jeho prvního výskytu, dostaneme nekonečnou posloupnost H délky ω, jejíž členy jsou navzájem různé prvky množiny x. Posloupnost H je skutečně nekonečná, neboť pro každé n obsahuje posloupnost G_n právě n navzájem různých členů. Formální definici posloupnosti H přenecháme čtenáři. Množina $\mathrm{Rng}(H)$ je spočetnou podmnožinou množiny x. □

Důsledek 6.17 (AC_ω)**.** *Množina x je nespočetná právě tehdy, když $\omega \prec x$.*

Důkaz. ($\Rightarrow$): Množina x je nekonečná, takže podle předchozí věty platí $\omega \preceq x$. Současně však $x \not\approx \omega$, neboť $x \npreceq \omega$ protože x není ani konečná, ani spočetná.

($\Leftarrow$): Kdyby byla množina x spočetná nebo konečná, tedy $x \preceq \omega$, pak by z Cantorovy–Bernsteinovy věty (protože $\omega \preceq x$) vyplývalo $x \approx \omega$, což je spor s $\omega \prec x$. □

Úloha 6.18. Dokažte z $\mathsf{AC}_\omega^{\mathsf{fin}}$, že sjednocení spočetně mnoha konečných množin je nejvýše spočetné.

Nápověda. Použijte trik s posloupnostmi z důkazu Věty 6.16. Ovšem v jakém pořadí napsat prvky dané konečné množiny co sjednocujete?

Úloha 6.19. Dokažte, že Königovo lemma vyplývá z tvrzení, že sjednocení spočetně mnoha konečných množin je nejvýše spočetné.

Nápověda. Klíčová myšlena je si uvědomit, že konečně se větvící stromy mají konečné levely (level stromu je množina vrcholů ve stejné vzdálenosti od kořene). Z našeho předpokladu pak vyplývá, že vrcholy daného stromu lze dobře uspořádat.

Úloha 6.20. Dokažte, že Königovo lemma implikuje $\mathsf{AC}_\omega^{\mathsf{fin}}$.

Nápověda. Pro daný soubor konečných množin $\langle A_i \mid i \in \omega \rangle$ definujte zakořeněný strom T, jehož vrcholy odpovídají částečným selektorům tohoto souboru.

6.5 Princip maximality

Axiom výběru je ekvivalentní s řadou tvrzení; jedno z nejužitečnějších mimo teorii množin je Zornovo lemma, také známé jako princip maximality.

Definice 6.21 (Řetězec)**.** Nechť $(A, \leq)$ je uspořádaná množina. Podmnožinu $B \subseteq A$ nazveme *řetězcem* v A, je-li B lineárně uspořádaná relací $\leq$.

Axiom 6.22 (Princip maximality PM)**.** Nechť $(A, \leq)$ je neprázdná uspořádaná množina, kde každý řetězec je shora omezený. Potom A obsahuje maximální prvek.

Poznámka. Princip maximality se často používá pro uspořádání $(A, \subseteq)$, kde $A \subseteq \mathcal{P}(x)$. Pak pro řetězec $B \subseteq A$ stačí ukázat, že $\bigcup B \in A$, jelikož $\bigcup B$ je horní mez, dokonce supremum, množiny B vzhledem k inkluzi.

Také existuje ekvivalentní, parametrizovaná verze principu maximality:

Axiom 6.23 (PPM)**.** Nechť $(A, \leq)$ je neprázdná uspořádaná množina, kde každý řetězec je shora omezený. Potom pro každé $a \in A$ existuje maximální prvek b množiny A takový, že $a \leq b$.

Pozorování 6.24. PM $\iff$ PPM.

Důkaz. Parametrizovanou verzi získáme z té normální tím, že se budeme dívat pouze na $A' \coloneqq \{b \in A \,|\, b \geq a\}$. Opačný směr zjevně platí. $\square$

Zmíníme ještě jednu ekvivalentní formulaci principu maximality, tentokrát přes suprema.

Axiom 6.25 (PMS)**.** Nechť $(A, \leq)$ je neprázdná uspořádaná množina, kde každý řetězec má supremum. Potom pro každé $a \in A$ existuje maximální prvek b množiny A takový, že $a \leq b$.

Úloha 6.26. Dokažte, že PM $\iff$ PPS.

Nápověda. Směr PM $\Rightarrow$ PPS by měl být zřejmý. Pro opačný směr uvažte množinu $\mathcal{R}$ všech řetězců dané množiny $(A, \leq)$, uspořádanou inkluzí. Podle poznámky na začátku této sekce, $\mathcal{R}$ splňuje předpoklad PMS.

Přechodem k opačnému uspořádání $(A, \geq)$ dostáváme z principu maximality princip minimality:

Pozorování 6.27. PM $\iff$ *Pokud $(A, \leq)$ je neprázdná uspořádaná množina, kde každý řetězec je zdola omezený, potom pro každé $a \in A$ existuje minimální prvek b množiny A takový, že $b \leq a$.*

Úloha 6.28. Pomocí principu maximality dokažte, že každý graf G má kostru.

Nápověda. Uvažte množinu všech podgrafů G co jsou stromy, uspořádanou inkluzí.

Úloha 6.29 (Szpilrajnova věta)**.** Pomocí principu maximality dokažte, že každé částečné uspořádání na množině A lze rozšířit na lineární uspořádání na A.

Nápověda. Uvažte množinu všech částečných uspořádání na A, uspořádanou inkluzí.

Úloha 6.30. Předpokládejte axiom výběru a uvažte následující zobecnění dobrých uspořádání. Připomeňme, že *kvaziuspořádání* na množině A je reflexivní, tranzitivní relace $\leq$. Pokud pro prvky $x, y \in A$ platí $x \leq y$ a zároveň $y \leq x$, pak píšeme $x \equiv y$ a říkáme, že jsou *ekvivalentní*. Pokud všechny ekvivalentní prvky ztotožníme (formálně uvážíme třídy ekvivalence $\equiv$), získáme částečně uspořádanou množinu $A/\equiv$.

Ukažte, že následující tvrzení jsou pro kvaziuspořádání $\leq$ na A ekvivalentní:

(1) Každá neprázdná podmnožina B uspořádané množiny $A/\equiv$ obsahuje alespoň jeden, ale pouze konečně mnoho minimálních prvků.

(2) Každé rozšíření $\leq^+$ uspořádání $\leq$ na $A/\equiv$, které je lineární, je dobré.

(3) A neobsahuje žádné nekonečné antiřetězce (podmnožiny vzájemně neporovnatelných prvků) ani žádné nekonečné klesající řetězce $x_0 > x_1 > x_2 > \cdots$, kde $x > y$ značí, že $y \leq x$ a zároveň $y \not\equiv x$.

Říkáme, že $\leq$ je *dobré kvaziuspořádání* množiny A.

Nápověda. Ukažte implikace (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). Pro implikaci (2) $\Rightarrow$ (3) by se mohl hodit výsledek předchozí úlohy.

6.6 Princip trichotomie

Axiom 6.31 (Princip trichotomie)**.** Pro libovolné dvě množiny x a y platí buď $x \preceq y$ nebo $y \preceq x$.

Věta 6.32. *Princip maximality implikuje princip trichotomie.*

Důkaz. Nejprve si připomeňme, že inverzní zobrazení k prostému zobrazení je prosté. Nyní nechť x, y jsou množiny, chceme sestrojit prosté zobrazení x do y, nebo y do x. Definujme množinu

$$P \coloneqq \{f \mid f \text{ je prosté zobrazení} \wedge \mathrm{Dom}(f) \subseteq x \wedge \mathrm{Rng}(f) \subseteq y\}.$$

Všimněme si, že uspořádaná množina $(P, \subseteq)$ splňuje podmínky principu maximality, jelikož sjednocení řetězce prostých zobrazení je prosté zobrazení. Nechť g je nějaký maximální prvek P. Kdyby obě množiny $x \setminus \mathrm{Dom}(g)$ a $y \setminus \mathrm{Rng}(g)$ byly neprázdné, tak by g šlo rozšířit o další dvojici, což je spor s maximalitou g. Proto buď $\mathrm{Dom}(g) = x$ a potom $x \preceq y$, nebo $\mathrm{Rng}(g) = y$ a potom $y \preceq x$. $\square$

Úloha 6.33. Ukažte z principu trichotomie, že každá nekonečná množina x má spočetnou podmnožinu; tedy, že $\omega \preceq x$.

Poznámka. Tohle umíme pouze za pomoci axiomu spočetného výběru, viz Sekce 6.4.

6.7 Princip dobrého uspořádání

Princip dobrého uspořádání (anglicky well-ordering principle) je tvrzení, že každou množinu lze dobře uspořádat. Byl jedním ze základních přesvědčení Cantora, avšak nepodařilo se mu jej dokázat. Tento problém slavně vyřešil v roce 1904 Ernst Zermelo. Zermelo jako první explicitně formuloval axiom výběru, který rozpoznal jako princip, jejž Cantor (a mnozí další matematici) v řadě důkazů implicitně používali. Následně ukázal, že axiom výběru a princip dobrého uspořádání jsou ekvivalentní. Proto se tomuto principu dnes občas říká Zermelova věta.

Axiom 6.34 (Princip dobrého uspořádání WO)**.** Každou množinu lze dobře uspořádat.

Věta 6.35. *Princip dobrého uspořádání implikuje axiom výběru.*

Důkaz. Nechť x je množina splňující $x \neq \varnothing$ a $\varnothing \notin x$. Chceme sestrojit selektor $f : x \to \bigcup x$. Podle WO existuje dobré uspořádání $\leq$ na $\bigcup x$ a každá $y \in x$ je neprázdná podmnožina $\bigcup x$, tedy má nejmenší prvek vůči $\leq$. Selektor f definujeme jako $f : y \mapsto \min_{\leq}(y)$. $\square$

Úloha 6.36. Dokažte, že princip maximality implikuje princip dobrého uspořádání.

Nápověda. Pro danou množinu X, kterou chceme dobře uspořádat, uvažte množinu

$$\mathcal{W} \coloneqq \{(A, <_R) \mid R \text{ is a well-order on } A \subseteq X\},$$

uspořádanou jako $(A, <_R) \sqsubset (B, <_S)$ pokud B prodlužuje A. Tedy pokud $A \subset B$, relace R je restrikce S na množinu A, a navíc A je dolní podmnožina B.

7 Ordinální čísla

Ordinální čísla představují jedno z možných zobecnění přirozených čísel. Intuitivně reprezentují *typy dobrých uspořádání.* Představme si, že chceme očíslovat prvky nějaké dobře uspořádané množiny: nejmenšímu prvku přiřadíme číslo 0, následujícímu číslo 1, a tak dále. *Typem* tohoto dobrého uspořádání je pak první číslo, které jsme již nemuseli použít. Co se však stane, když nám dojdou čísla?

Uvažme například následující dobré uspořádání přirozených čísel:

$$1 \prec 2 \prec 3 \prec 4 \prec 5 \prec \cdots \prec 0.$$

Budeme-li prvky číslovat zleva doprava, využijeme všechna přirozená čísla pro úsek $1 \prec 2 \prec \cdots$, takže pro prvek 0 nám již žádné přirozené číslo nezbude. Právě proto zavádíme ordinální čísla: prvku 0 přiřadíme „číslo“ ω a typ tohoto uspořádání tak bude ordinální číslo $\omega + 1$.

Podobně, dobré uspořádání

$$0 \prec 2 \prec 4 \prec 6 \prec \cdots \prec 1 \prec 3 \prec 5 \prec 7 \prec \cdots$$

má typ $\omega + \omega$, protože všechna přirozená čísla n použijeme k očíslování sudých čísel, a poté všechna ordinální čísla tvaru $\omega + n$, která zatím chápeme intuitivně, použijeme k očíslování lichých čísel.

Poznámka. Před pokračováním ve čtení zbytku této sekce by pro získání intuice mohlo být užitečné si nejprve rychle projít Podsekci 7.7, protože formální definice ordinálních čísel může být z zprvu trochu nejasná.

7.1 Tranzitivní třídy

Definice 7.1. Třída X je *tranzitivní*, pokud pro každé $x \in X$ platí $x \subseteq X$. Nebo ekvivalentně, pokud pro každé $x \in X$ a $y \in x$ platí $y \in X$.

Pozorování 7.2. *Třída X je tranzitivní $\iff \bigcup X \subseteq X$.*

Lemma 7.3. *Vlastnosti tranzitivních tříd.*

(1) *Jsou-li X a Y tranzitivní třídy, pak $X \cap Y$ a $X \cup Y$ jsou také tranzitivní.*

(2) *Je-li každá množina $x \in X$ tranzitivní, tak $\bigcap X$ a $\bigcup X$ jsou tranzitivní třídy.*

(3) *Je-li každá množina $x \in X$ tranzitivní, pak je relace $\in$ tranzitivní na třídě X.*

(4) *Je-li X tranzitivní třída a relace $\in$ je tranzitivní na X, tak každá množina $x \in X$ je tranzitivní.*

Důkaz. Všechno je to hraní si s definicemi.

(1) Plyne přímo z definice.

(2) Ukážeme pro průnik; suma se dokazuje podobně. Nechť $y \in z \in \bigcap X$, chceme ukázat, že $y \in \bigcap X$. Jelikož $z \in \bigcap X$, tak $z \in x$ pro nějakou $x \in X$. Protože je x tranzitivní, tak z $y \in z \in x$ máme $y \in x$, tedy $y \in \bigcap X$.

(3) Nechť $x, y, z \in X$ splňují $z \in y \in x$, chceme $z \in x$. To platí, protože x je tranzitivní.

(4) Nechť $z \in y \in x \in X$, chceme $z \in x$. Protože X je tranzitivní, tak $z \in y \in X$, a tudíž také $z \in X$. Jelikož $\in$ je tranzitivní na X a $x, y, z \in X$, tak $z \in x$. $\square$

Důsledek 7.4. *Je-li X tranzitivní třída, potom:*

$$\textit{Relace } \in \textit{ je tranzitivní na } X \iff \textit{každá množina } x \in X \textit{ je tranzitivní.}$$

Důkaz. Vyplývá z kombinace (3) a (4). □

Úloha 7.5. Najděte tranzitivní množinu X, na níž relace náležení $\in$ není tranzitivní.

7.2 Definice ordinálních čísel

Definice 7.6 (Von Neumann)**.** Množina x je *ordinální číslo*, pokud

(i) x je tranzitivní množina, a zároveň

(ii) relace náležení $\in$ je dobré ostré uspořádání na x.

Třídu všech ordinálních čísel značíme On

Úloha 7.7. Projděte si znovu Sekci 5.4 a přesvědčte se, že každé přirozené číslo $n \in \omega$ i samotná množina všech přirozených čísel ω jsou ordinální čísla.

Úloha 7.8. Najděte množinu x, která *není* tranzitivní, ale relace náležení $\in$ je dobré ostré uspořádání na x.

Lemma 7.9. On *je tranzitivní třída.*

Důkaz. Ukážeme, že každé $y \in x \in \mathrm{On}$ je také ordinální číslo. Protože x je ordinál, tak relace $\in$ je na x dobré uspořádání, speciálně je tedy tranzitivní. Podle Lemma 7.3 (4) je potom $y \in x$ tranzitivní množina. Ještě musíme ukázat, že $\in$ je dobré ostré uspořádání na y. Ale to je, jelikož $y \subseteq x$ (protože $y \in x$ a x je tranzitivní množina) a vlastnost „být dobré ostré uspořádání“ je dědičná. □

7.3 Uspořádání ordinálních čísel relací náležení

Lemma 7.10. *Pro každá dvě $x, y \in \mathrm{On}$ platí*

(i) $x \notin x$,

(ii) $x \cap y \in \mathrm{On}$,

(iii) $x \in y \iff x \subset y$.

Důkaz. (i) Kdyby $x \in x$ tak bychom dostali spor s tím, že $\in$ je antireflexivní na x.

(ii) Podle Lemma 7.3 (1) je $x \cap y$ tranzitivní množina a je dobře (ostře) uspořádaná relací $\in$, protože to je podmnožinou ordinálu x.

(iii) Směr '$\Rightarrow$' z tranzitivity y a (i). Pro opačný směr nechť $x \subset y$. Protože y je dobře uspořádaná, tak $\emptyset \neq y \setminus x \subseteq y$ má nejmenší prvek vůči $\in$, označme jej z. Ukážeme, že $z = x$. Nejprve inkluze $x \subseteq z$. Nechť $u \in x$, protože $x \subseteq y$, tak $u \in y$. Protože y je ordinál, tak $\in$ je lineární na y, takže prvky u a z můžeme porovnat. Jsou tři možnosti:

(a) $u \in z$, to jsme chtěli.

(b) $u = z$, ale $z \notin x$, takže $u \notin x$, což je spor.

(c) $z \in u$, z tranzitivity x máme $z \in u \in x \implies z \in x$, což je opět spor.

Nyní inkluze $z \subseteq x$. Nechť $u \in z$, podle tranzitivity y máme $u \in z \in y \implies u \in y$, ukážeme $u \in x$. Kdyby $u \notin x$, tak u je menší prvek v doplňku $y \setminus x$ než z, což je spor s minimalitou z. $\square$

Věta 7.11. *Relace $\in$ je dobré ostré uspořádání na* On.

V důkazu této věty budeme hojně používat předchozí lemma, a na jeho části se budeme odkazovat jako (i), (ii), a (iii).

Důkaz. Podle (i) je $\in$ antireflexivní na On. Navíc, protože každé $x \in \mathrm{On}$ je tranzitivní množina, tak podle části (3) Lemma 7.3 je $\in$ tranzitivní na On. Dohromady to znamená, že $\in$ je ostré uspořádání na On.

Dále ukážeme, že relace $\in$ trichotomická na On, tudíž to je lineární (ostré) uspořádání. Nechť $x, y \in \mathrm{On}$, chceme je porovnat. Podívejme se na množinu

$$z := x \cap y.$$

Podle (ii) je $z \in \mathrm{On}$, a navíc tvrdíme, že $z = x$ nebo $z = y$. Kdyby $z \subset x$ a $z \subset y$, pak podle (iii) $z \in x$ a $z \in y$, čili $z \in z$, což je spor s (i). Nyní rozbor případů:

(a) $x = y$, pak jsme skončili, jinak

(b) $z = x$ a $z \subset y$, pak $x \in y$ podle (iii),

(c) $z = y$ a $z \subset x$, pak $y \in x$ podle (iii).

Dobrost zdůvodníme podobně jako pro ω. Nechť $A \subseteq \mathrm{On}$ je neprázdná množina ordinálů a $x \in A$. Není-li x minimální,[10] označme $B := x \cap A$. Zřejmě $B \neq \emptyset$, jinak by x bylo minimální. Jelikož $B \subseteq x$ a x je ordinální číslo, tak je množina B dobře (ostře) uspořádaná relací $\in$ a má nejmenší prvek y. Tvrdíme, že y je minimální také v A. Kdyby ne, tak existuje nějaké $z \in y$ takové, že $z \in A$. Ale $y \in x$, takže z tranzitivity množiny x je $z \in x$. Tedy $z \in B$, což je spor s minimalitou y. $\square$

Poznámka. Tento argument dokonce ukazuje, že každá neprázdná *podtřída* $A \subseteq \mathrm{On}$ má minimální prvek.

Důsledek 7.12. On *je vlastní třída.*

Důkaz. Podle Lemma 7.9 je On tranzitivní třída, a podle předchozí věty je dobře ostře uspořádaná relací $\in$. Tedy kdyby On byla množinou, tak by to byl ordinál, tedy $\mathrm{On} \in \mathrm{On}$, což je spor s antireflexibilitou $\in$ na On. $\square$

Věta 7.13. *Je-li X tranzitivní vlastní třída, která je dobře ostře uspořádaná relací náležení $\in$, potom $X = \mathrm{On}$.*

Důkaz. Jelikož je X tranzitivní, tak pokud $x \in X$, potom $x \subseteq X$. Protože X je dobře uspořádaná relací $\in$, tak z dědičnosti je x také dobře uspořádaná. Navíc jelikož je $\in$ tranzitivní na X, tak podle části (4) Lemma 7.3 je x tranzitivní množina. Proto je x ordinální číslo, čili $X \subseteq \mathrm{On}$.

Pro spor nechť platí pouze ostrá inkluze a $x \in \mathrm{On} \setminus X$. Ukážeme, že $X \subseteq x$, což je spor s tím, že X je vlastní třída. Nechť $y \in X$. Kdyby $y \notin x$, tak z trichotomie $\in$ na On buď $x = y$, nebo $x \in y$, a potom $x \in X$ protože X je tranzitivní. Každopádně $x \in X$, což je spor s naší volbou x. $\square$

[10] Minimální a nejmenší je pro lineární uspořádání to samé.

Tato sekce se nesla v duchu zobecňování výsledků Sekce 5.4 z přirozených čísel na ordinální čísla. Ještě vyslovíme (bez důkazu) ordinální ekvivalent Věty 5.49.

Věta 7.14. *Pokud je $(W, <_R)$ dobře (ostře) uspořádaná vlastní třída taková, že pro každé $x \in W$ je dolní třída $(\leftarrow, x]$ množinou, potom je $(W, <_R)$ izomorfní* $(\mathrm{On}, \in)$.

Důsledek 7.15. *Každý vlastní dolní podtřída $A \subset \mathrm{On}$ je ordinální číslo.*

Důkaz. Nejprve ukážeme, že A je tranzitivní: pokud $\alpha \in \beta \in A$, neboli $\alpha < \beta \in A$, pak $\alpha \in A$, jelikož A je dolní třída. Také je dobře ostře uspořádaná relací $\in$, protože $A \subseteq \mathrm{On}$ (z dědičnosti). Zbývá ukázat, že A je množina. Kdyby byla vlastní třídou, tak podle předchozí věty platí $A = \mathrm{On}$, což je není pravda, spor. □

7.4 Vlastnosti ordinálních čísel

Ordinální čísla od teď budeme značit písmeny ze začátku řecké abecedy $\alpha, \beta, \gamma, \dots$, a budeme psát $\alpha < \beta$ namísto $\alpha \in \beta$ a $\alpha \leq \beta$ namísto $\alpha \in \beta \vee \alpha = \beta$.

Je dobré si uvědomit, že jelikož $\beta < \alpha$ je to samé co $\beta \in \alpha$, tak ordinální číslo α je přesně množinou všech menších (vůči $<$) ordinálů $\beta < \alpha$, a navíc

$$\beta \leq \alpha \iff \beta \subseteq \alpha \implies \beta \preceq \alpha,$$

podle Lemma 7.10.

Pozorování 7.16. *Konečná ordinální čísla jsou právě přirozená čísla.*

Důkaz. Předpokládejme, že $\alpha \in \mathrm{On}$ je konečná množina, ale $\alpha \notin \omega$. Z trichotomie relace $\in$, respektive $<$, na On musí platit $\omega \leq \alpha$, a podle naší předchozí diskuze $\omega \preceq \alpha$, tedy α není konečná. □

Dále poznamenejme, že jelikož ordinální čísla jsou dobře uspořádaná, tak každá neprázdná množina ordinálních čísel $A \subseteq \mathrm{On}$ má supremum

$$\sup(A) = \min\{\alpha \in \mathrm{On} \mid (\forall \beta \in A)\alpha \geq \beta\}.$$

Za chvíli dokážeme velmi užitečné tvrzení, které říká, že

$$\sup(A) = \bigcup A.$$

Pozorování 7.17. *ω je nejmenší (vůči $<$) nekonečné ordinální číslo.*

Důkaz. Podle Pozorování 7.16 je ω množinou všech konečných ordinálních čísel, čili nejmenší nekonečné ordinální číslo je $\sup(\omega)$. Ale $\sup(\omega) = \bigcup \omega$, a je snadné ověřit (například pomocí Lemma 5.43), že $\bigcup \omega = \omega$. □

Lemma 7.18. *Pro množiny ordinálních čísel platí následující.*

(a) *Množina $A \subseteq \mathrm{On}$ je ordinálním číslem $\iff$ A je tranzitivní.*

(b) *Pokud je $A \subseteq \mathrm{On}$ množina, pak $\sup(A) = \bigcup A$.*

(c) *Pokud je $A \subseteq \mathrm{On}$ neprázdná třída, pak $\min(A) = \bigcap A$.*

Důkaz.

(a) Směr '$\Rightarrow$' z definice. Pro opačný směr nechť A je tranzitivní, potřebujeme aby $\in$ bylo dobré ostré uspořádání na A. Ale to je, protože $\in$ je dobré ostré uspořádání na On, takže z dědičnosti i na $A \subseteq \mathrm{On}$.

(b) Podle Lemma 7.3 je $\bigcup A$ tranzitivní, protože všechny prvky A jsou tranzitivní, tedy podle (a) je $\beta \coloneqq \bigcup A$ ordinál. Tvrdíme, že je navíc supremum A. Pro každé $\alpha \in A$ platí $\alpha \subseteq \bigcup A = \beta$, tedy $\alpha \subseteq \beta \implies \alpha \leq \beta$, takže β je horní mez množiny A. Zbývá ukázat, že žádné $\gamma < \beta$ horní mez být nemůže. Pokud $\gamma < \beta$, neboli $\gamma \in \bigcup A$, tak existuje $\alpha \in A$ takové, že $\gamma \in \alpha$, neboli $\gamma < \alpha$, tedy γ není horní mezí A.

(c) Podle Věty 7.11 (a poznámky pod jejím důkazem) má A nejmenší prvek A. Pro libovolné $\beta \in A$ platí $\alpha \leq \beta$, takže $\alpha \subseteq \beta$, a proto $\alpha \subseteq \bigcap A$. Jelikož $\alpha \in A$, platí také $\bigcap A \subseteq \alpha$. □

7.5 Typy dobře uspořádaných množin

Jsou-li dvě množinové relace izomorfní, tak se podstatně neliší, přestože popisují vztahy mezi prvky různých množin. Dává proto smysl uvažovat o ekvivalenci „být izomorfní" na třídě všech relací. Je snadné nahlédnout, že ekvivalenční třídy této ekvivalence jsou vlastní třídy, proto nemůžeme udělat rozklad. Ale bylo by hezké, kdybychom mohli pro každou ekvivalenční třídu sestrojit nějakého reprezentanta, abychom pak mohli vše týkající se relací daného typu dokazovat na tomto reprezentantovi.

Pro relace tvořící dobrá uspořádání jsou tito reprezentanti právě ordinální čísla.

Pozorování 7.19. *Žádná dvě ordinální čísla nejsou izomorfní, a pokud je ordinální číslo $(\alpha, <)$ izomorfní s nějakou dobře uspořádanou množinou $(W, <_R)$, potom je tento izomorfismus jednoznačně určený.*

Důkaz. Snadný důsledek Věty 4.47. □

Věta 7.20 (O typu dobrého uspořádání)**.** *Každá dobře uspořádaná množina $(W, <_R)$ je izomorfní s jednoznačně určeným ordinálním číslem $(\alpha, <)$. Ordinální číslo α nazýváme* typem *dobře uspořádané množiny $(W, <_R)$.*

Nástin důkazu. Nechť X je množina všech prvků $x \in W$ takových, že počáteční úsek $(\leftarrow, x)$ je izomorfní s nějakým ordinálním číslem, které označíme α_x. Podle axiomu nahrazení tvoří množina všech těchto ordinálních čísel množinu S. Lze ověřit, že X je dolní podmnožina W a S je dolní podmnožina On. Z toho se dá ukázat, že S musí samo být ordinálním číslem, které označíme α. Zobrazení $x \mapsto \alpha_x$ přirozeně určuje izomorfismus mezi X a α. Pokud $X = W$ tak jsme vyhráli. Jinak podle Lemma 4.45 platí $X = (\leftarrow, c)$ pro nějaký prvek $c \in W$. Jenže potom z definice X máme $c \in X$ a $\alpha_c = \alpha \in S = \alpha$, což je spor. □

7.6 Transfinitní indukce a rekurze

V matematice často používáme matematickou indukci na přirozených číslech. Také je užitečná rekurze, například $f(0) = 1$ a $f(n) = n \cdot f(n-1)$, k definování funkcí. Nyní ukážeme, jak tyto principy zobecnit na všechna ordinální čísla.

Lemma 7.21. *Pokud $\alpha \in \mathrm{On}$, pak $\alpha \cup \{\alpha\}$ je nejmenší ordinální číslo větší než α.*

Důkaz. Nejprve ukážeme, že to je ordinální číslo. Protože je α tranzitivní, tak $\alpha \cup \{\alpha\}$ je taky tranzitivní (snadný rozbor případů). Protože $\alpha \subseteq \mathrm{On}$, tak dokonce je $\alpha \cup \{\alpha\}$ tranzitivní množina ordinálních čísel, podle Lemma 7.18 je tedy také ordinálním číslem. Nyní, že je nejmenší větší než α. Je-li $\beta < \alpha \cup \{\alpha\}$, neboli $\beta \in \alpha \cup \{\alpha\}$, pak $\beta \in \alpha$ nebo $\beta = \alpha$, tedy $\beta \leq \alpha$. □

Definice 7.22. Je-li α ordinální číslo, tak ordinál $\alpha + 1 \coloneqq \alpha \cup \{\alpha\}$ nazýváme *následníkem* α, a ordinál α nazýváme *předchůdcem* $\alpha + 1$.

Definice 7.23. Ordinální číslo α je *izolované*, pokud $\alpha = 0$ nebo $\alpha = \beta + 1$ pro nějaký ordinál β, jinak je α *limitní*.

Příklad. Příklady izolovaných ordinálních čísel jsou všechna přirozená čísla nebo ordinální čísla $\omega + 1$, $\omega \cdot 2 + 7$ a $\omega^\omega + 2$, která zavedeme později. Příklady limitních ordinálních čísel jsou ω, $\omega + \omega$ nebo $\omega \cdot \omega$.

Věta 7.24 (Princip transfinitní indukce)**.** *Nechť $A \subseteq \mathrm{On}$ je třída taková, že pro každé ordinální číslo $\alpha \in \mathrm{On}$ platí $\alpha \subseteq A \Rightarrow \alpha \in A$, neboli*

$$(\forall \beta < \alpha)(\beta \in A) \implies (\alpha \in A). \tag{7.1}$$

Potom $A = \mathrm{On}$.

Ekvivalentně, nechť $\varphi(x)$ je vlastnost splňující, že pro každé ordinální číslo α platí:

Jestliže $\varphi(\beta)$ platí pro všechna $\beta < \alpha$, pak platí i $\varphi(\alpha)$.

Pak $\varphi(\alpha)$ platí pro všechna ordinální čísla $\alpha \in \mathrm{On}$.

Důkaz. Předpokládejme, že existuje $\gamma \in \mathrm{On} \setminus A$, a položme

$$S \coloneqq \{\alpha \leq \gamma \mid \alpha \notin A\}.$$

Protože ordinální čísla jsou dobře uspořádaná, množina S má nejmenší prvek α. Jelikož každé $\beta < \alpha$ patří do A, plyne z (7.1), že $\alpha \in A$, což je spor.

Ekvivalenci obou formulací snadno získáme volbou třídy $A = \{x \mid \varphi(x)\}$, resp. vlastnosti $\varphi(x) \equiv (x \in A)$. □

Princip transfinitní indukce lze také formulovat zvlášť pro izolované a limitní ordinály, čímž získáme tvar bližší obvyklé matematické indukci na přirozených číslech.

Věta 7.25 (Princip transfinitní indukce II)**.** *Nechť $A \subseteq \mathrm{On}$ je třída splňující*

(i) $0 \in A$,

(ii) $\alpha \in A \implies \alpha + 1 \in A$, *. . . jedná se o běžnou indukci na ω,*

(iii) *je-li α limitní ordinální číslo a pro všechna $\beta < \alpha$ platí $\beta \in A$, pak $\alpha \in A$.*

Potom $A = \mathrm{On}$. Toto tvrzení opět lze snadno přepsat pomocí vlastnosti $\varphi(x)$.

Důkaz. Stačí ukázat, že tyto tři předpoklady implikují podmínku (7.1). Nechť tedy α je ordinální číslo takové, že pro všechna $\beta < \alpha$ platí $\beta \in A$.

Je-li $\alpha = 0$, pak $\alpha \in A$ podle (i). Je-li $\alpha \neq 0$ izolované, tedy existuje-li $\beta < \alpha$ takové, že $\alpha = \beta + 1$, pak $\beta \in A$, a tudíž $\alpha \in A$ podle (ii). Je-li α limitní ordinální číslo, dostáváme $\alpha \in A$ přímo z (iii). □

Pomocí transfinitní indukce můžeme dokazovat vlastnosti různých nekonečných struktur. Naproti tomu, transfinitní rekurze nám umožňuje konstruovat různé nekonečně složité struktury a definovat funkce rekurzivním způsobem.

Věta 7.26 (O konstrukci transfinitní rekurzí)**.** *Je-li $G : \mathbf{V} \to \mathbf{V}$ zobrazení, pak existuje právě jedno zobrazení $F : \mathrm{On} \to \mathbf{V}$ splňující*

$$F(\alpha) = G(F \restriction \alpha). \tag{7.2}$$

Jinými slovy, hodnotu funkce v ordinálním čísle α je určená na základě ordinálů $\beta < \alpha$ a hodnot funkce F v těchto ordinálech.

Poznámka. Toto tvrzení se může zdát poněkud podezřelé, protože na první pohled tvrdí, že pro každou třídu G existuje třída F s určitou vlastností. Ale přitom nám jazyk ZFC neumožňuje kvantifikovat přes třídy. Ve skutečnosti proto jde o schéma vět, jedna pro každou konkrétní třídu G. Třídu F navíc nekvantifikujeme, protože následující důkaz ji explicitně zkonstruuje.

Poznámka. Díky tomu, jak je definice $F(\alpha)$ pomocí $(\beta, F(\beta))$ pro všechna $\beta < \alpha$ obecná, můžeme funkce definovat mnoha dalšími typy rekurze. Například:

- $F(\alpha) = G\big(F[\alpha]\big) = G\big(\{F(\beta) \mid \beta < \alpha\}\big)$,
- $G : \mathrm{On} \times \mathbf{V} \to \mathbf{V}$ a $F(\alpha) = G(\alpha, F \restriction \alpha)$,
- Je-li $\alpha = \beta + 1$ izolované ordinální číslo, pak $F(\alpha) = G_1(F(\beta))$, zatímco pro limitní ordinální čísla je $F(\alpha) = G_2(F[\alpha])$. Toto je asi nejšikovnější formulace.

Důkaz. Definujme A jako třídu všech „množinových aproximací“ zobrazení F. Jde o množinová zobrazení f, jejichž definičním oborem je nějaké ordinální číslo β, a pro všechna $\alpha < \beta$ platí $f(\alpha) = G(f \restriction \alpha)$. Nyní definujeme F jako $F \coloneqq \bigcup A$. Je zřejmé, že $F \subseteq \mathrm{On} \times \mathbf{V}$. Ukážeme, že $F : \mathrm{On} \to \mathbf{V}$ je jediné zobrazení splňující (7.2).

Nejprve ukážeme, že se aproximace F shodují. Nechť $f, f' \in A$ a $\alpha \in \mathrm{Dom}(f) \cap \mathrm{Dom}(f')$. Tvrdíme, že $f(\alpha) = f'(\alpha)$. Podle Lemma 7.10 je $\mathrm{Dom}(f) \cap \mathrm{Dom}(f')$ ordinál δ. Pro spor předpokládejme, že $\alpha \in \delta$ je nejmenší ordinál, pro který $f(\alpha) \neq f'(\alpha)$. Pak $f \restriction \alpha = f' \restriction \alpha$, takže $f(\alpha) = G(f \restriction \alpha) = G(f' \restriction \alpha) = f'(\alpha)$, což je spor.

Za druhé ověříme, že F splňuje (7.2); tedy že pro všechna $\alpha \in \mathrm{Dom}(F)$ platí $F(\alpha) = G(F \restriction \alpha)$. Nechť $\alpha \in \mathrm{Dom}(F)$. Tento prvek leží v definičním oboru díky nějakému $f \in A$ splňujícímu $\alpha \in \mathrm{Dom}(f)$ a $f(\alpha) = G(f \restriction \alpha)$. Zároveň platí $F(\alpha) = f(\alpha)$ a $F \restriction \alpha = f \restriction \alpha$. Spojením těchto rovností tedy dostáváme $F(\alpha) = G(F \restriction \alpha)$.

Dále ukážeme, že $\mathrm{Dom}(F) = \mathrm{On}$. Nejprve dokážeme, že $\mathrm{Dom}(F)$ je dolní podtřída On. Předpokládejme, že $\alpha \in \mathrm{Dom}(F)$; tento prvek tam leží díky nějakému $f \in A$ s definičním oborem $\delta > \alpha$. Je-li $\beta < \alpha$, pak také $\beta \in \delta$, a tudíž $\beta \in \mathrm{Dom}(F)$.

Podle Důsledku 7.15 platí buď $\mathrm{Dom}(F) = \mathrm{On}$, což chceme dokázat, nebo $\mathrm{Dom}(F) = \gamma \in \mathrm{On}$. Předpokládejme pro spor, že $\mathrm{Dom}(F) = \gamma$. Pak je F množina, protože $\mathrm{Dom}(F)$ je množina, $\mathrm{Rng}(F)$ je množina (s využitím axiomu nahrazení) a $F \subseteq \mathrm{Dom}(F) \times \mathrm{Rng}(F)$. To ale znamená, že $F \in A$, protože jeho definičním oborem je ordinál a již jsme ověřili, že splňuje vlastnost rekurzivní definice.

Nyní, když $F \in A$, definujeme o něco „delší“ funkci $F_1 \coloneqq F \cup \{(\gamma, G(F))\}$; všimněme si, že $F = F_1 \restriction \gamma$. Dále si všimněme, že $F_1 \in A$, protože $\mathrm{Dom}(F_1) = \gamma + 1$ je ordinál a F_1 jsme definovali tak, aby splňovalo vlastnost rekurzivní definice. Protože $F = \bigcup A$, implikuje to $F_1 \subseteq F$, ale pak $\gamma \in \mathrm{Dom}(F_1) \subseteq \mathrm{Dom}(F) = \gamma$, což je spor. Ukázali jsme, že $\mathrm{Dom}(F) = \mathrm{On}$.

Nakonec dokážeme jednoznačnost F. Pro spor předpokládejme, že existuje jiné zobrazení $F' \neq F$ splňující tvrzení této věty. Protože je $(\mathrm{On}, <)$ dobře uspořádaná, můžeme vzít nejmenší ordinál α, pro který $F(\alpha) \neq F'(\alpha)$. Proto $F \restriction \alpha = F' \restriction \alpha$, a tedy $F(\alpha) = G(F \restriction \alpha) = G(F' \restriction \alpha) = F'(\alpha)$, což je spor. □

Věta 7.27. *Axiom výběru implikuje princip maximality.*

Důkaz. Nechť $(A, <_R)$ je neprázdná uspořádaná množina, kde má každý řetězec horní mez, a pro spor předpokládejme, že A nemá žádný maximální prvek. Potom každý řetězec $C \subseteq A$ má dokonce *striktní* horní hranici $x \in A$ splňující $x > c$ pro každé $c \in C$, jinak bychom měli maximální prvek.

Pomocí axiomu výběru získáme selektor g na $\mathcal{P}(A)$ a pro každý řetězec $C \subseteq A$ *vybereme* takovou striktní horní hranici $g(C) \in A$. Zvolíme libovolný prvek $a \in A$ a transfinitní rekurzí definujeme funkci $F : \mathrm{On} \to A$ jako $F(0) \coloneqq a$, a pro $\alpha > 0$ jako $F(\alpha) \coloneqq g(F[\alpha])$. Tohle je korektní díky tomu, že stále prodlužujeme řetězec začínající v a. Ze stejného důvodu je F prosté zobrazení z vlastní třídy On do množiny A, což je spor s axiomem nahrazení. □

Poznámka. Správně bychom měli funkci F definovat pomocí funkce $G : \mathbf{V} \to \mathbf{V}$. Tu můžeme definovat jako $G(\varnothing) \coloneqq a$, pro řetězec $C \subseteq A$ jako $G(C) \coloneqq g(C)$, a pro ostatní množiny $x \in \mathbf{V}$ třeba jako $G(x) \coloneqq \varnothing$.

Věta 7.28. *Axiom výběru implikuje princip dobrého uspořádání.*

Nástin důkazu. Nechť A je množina, a g selektor na $\mathcal{P}(A)$. Pomocí transfinitní rekurze sestrojíme dobré uspořádání množiny A. Definujeme funkci $f(0) \coloneqq g(A)$, $f(\beta) \coloneqq g(A \setminus f[\beta])$, takže pro β si z A vyberu nějaký prvek, který jsem ještě nepoužil. Vlastně si prvky té množiny A očíslujeme ordinálními čísly. Pro $a \in A$ označme jako α_a jednoznačně určený ordinál co jsme přiřadili prvku a. Nyní můžeme definovat dobré uspořádání R na A jako $a <_R b \iff \alpha_a < \alpha_b$. □

Poslední dvě věty, společně s Větou 6.32 a Úlohou 6.36, ukazují, že:

Věta 7.29. *Následující tvrzení jsou v* ZF *ekvivalentní.*

(1) *Axiom výběru.*

(2) *Princip dobrého uspořádání.*

(3) *Princip maximality.*

Úloha 7.30 (AC)**.** Dokažte, že každý vektorový prostor (i nekonečné dimenze) má bázi. Báze vektorového prostoru V je množina vektorů $B \subseteq V$ taková, že každá konečná podmnožina $A \subseteq B$ je lineárně nezávislá, a každý vektor $v \in V$ je možné vyjádřit jako lineární kombinaci konečně mnoha vektorů z B.

Nápověda. Zkuste to dvěma způsoby: můžete buď přímo z principu maximality, nebo pomocí transfinitní rekurze a axiomu výběru.

7.7 Ordinální aritmetika

Z toho, co jsme zatím o ordinálních číslech dokázali, možná není jasné, proč se jim říká ordinální *čísla*. Základy ordinální aritmetiky by tuto záhadu měly objasnit.[11]

Připomeňme, že *lexikografické uspořádání* kartézského součinu $A \times B$ dvou uspořádaných množin $(A, <_R)$ a $(B, <_S)$ je definováno jako

$$(a_1, b_1) <_L (a_2, b_2) \iff \begin{cases} a_1 < a_2, \text{ nebo} \\ a_1 = a_2 \wedge b_1 < b_2. \end{cases}$$

Pokud jsou A a B dobře uspořádané, pak je lex. uspořádání $A \times B$ také dobré.

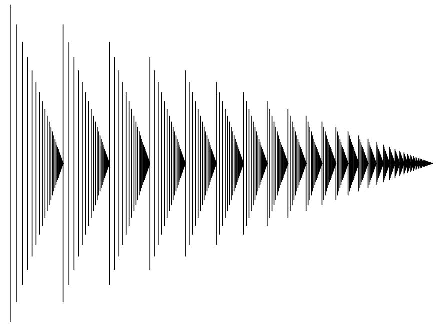
Definice 7.31. Pro ordinální čísla α a β definujeme ordinály

(a) $\alpha + \beta$ jako typ uspořádání množiny $(\{0\} \times \alpha) \cup (\{1\} \times \beta)$ při lexikografickém uspořádání,

(b) $\alpha \cdot \beta$ jako typ uspořádání množiny $\beta \times \alpha$ při lexikografickém uspořádání.

[11] Doporučuji také shlédnout následující video od Vsauce, které hezky ilustruje, jak z již existujících ordinálů konstruovat větší: `https://www.youtube.com/watch?v=SrU9YDoXE88`.

Všimněte si, že naše předchozí značení $\alpha \cup \{\alpha\}$ jako $\alpha + 1$ je s výše uvedenou definicí konzistentní. Můžeme si $\alpha+\beta$ představit jako hromádku zmenšujících se tyček očíslovaných pomocí prvků α, za kterou následuje další hromádka tyček, očíslovaná pomocí prvků β. Všimněme si, že v definici $\alpha \cdot \beta$ používáme $\beta \times \alpha$. Ordinál $\alpha \cdot \beta$ si lze představit tak, že vezmeme hromádku tyček očíslovanou pomocí β a každou tyčku nahradíme kopií α (hromádkou tyček očislovaných pomocí α).



Obrázek 1: Reprezentace ordinálu $\omega\cdot\omega$. Každá tyčka odpovídá ordinálu tvaru $\omega\cdot m+n$, kde m a n jsou přirozená čísla [4].

S touto intuicí by nemělo být překvapením, že ordinální sčítání a násobení obecně nejsou komutativní. Zřejmě $1 + \omega = \omega$, ale $\omega + 1 \neq \omega$. Co se týče násobení, uvažme $2 \cdot \omega$, typ uspořádání spočetně nekonečně mnoha kopií $\{0, 1\}$ poskládaných za sebou. To lze zjevně očíslovat pomocí ω, takže $2 \cdot \omega = \omega$. Ale $\omega \cdot 2$ je typ uspořádání dvou po sobě jdoucích kopií ω. Když se je pokusíme očíslovat pomocí prvků ω, vyčerpáme všechna $n \in \omega$ k označení první kopie, a pro druhou kopii budeme potřebovat další ordinály. Proto $\omega \cdot 2 > \omega$.

Pozorování 7.32. *Pro libovolné ordinály α, β, γ a přirozené číslo $n \in \omega$ platí, že*

(a) $\alpha + 0 = \alpha = 0 + \alpha, \qquad \alpha \cdot 0 = 0 = 0 \cdot \alpha, \qquad \alpha \cdot 1 = \alpha = 1 \cdot \alpha,$

(b) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma, \qquad \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma,$

(c) $\alpha \cdot 2 = \alpha + \alpha, \qquad \alpha \cdot 3 = \alpha + \alpha + \alpha, \qquad \alpha \cdot (n + 1) = \alpha \cdot n + \alpha.$

Definice 7.33. Pro ordinální čísla α a β definujeme ordinál α^β rekurzivně[12] jako

(i) $\alpha^0 := 1$,

(ii) $\alpha^{\beta+1} := \alpha^\beta \cdot \alpha$,

(iii) pokud je β limitní ordinál, pak $\alpha^\beta := \sup\{\alpha^\gamma \mid 0 < \gamma < \beta\}$.

Abychom získali trochu intuice, uvažme ordinál $\omega^2 = \omega \cdot \omega$. Ten reprezentuje několik kopií ω uspořádaných stejným způsobem jako ω. Pro konstrukci $\omega^3 = (\omega\cdot\omega)\cdot\omega$ vezmeme několik kopií ω^2 a uspořádáme je podle ω. Pokud tento proces zopakujeme ω-krát, dostaneme se až k ordinálu ω^ω. Můžeme pokračovat a získávat stále větší a větší ordinály, jako jsou $\omega^{(\omega^\omega)}$ nebo $\omega^{(\omega^{(\omega^\omega)})}$. Nakonec zkonstruujeme ordinál

$$\varepsilon_0 := \sup\left\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\right\},$$

který úzce souvisí s Peanovou aritmetikou. Může být překvapivé, že tento ordinál je stále spočetný a v jistém smyslu poměrně malý, i na spočetné ordinály.

Úloha 7.34. Zkuste zkonstruovat první nespočetný ordinál ω_1, nebo alespoň dokázat jeho existenci.

[12] Rozmyslete si, jak přesně zde formálně využíváme konstrukci transfinitní rekurzí.

8 Aplikace ordinálních čísel

Předvedeme si, že ordinální čísla jsou užitečná i mimo teorii množin.

8.1 Transfinitní rekurze v geometrie

Nejprve uvedeme dvě tvrzení, která je možné dokázat bez rekurze (zkuste to).

Úloha 8.1. $\mathbb{R}^3$ je sjednocením navzájem mimoběžných přímek.

Úloha 8.2. $\mathbb{R}^3$ je sjednocením navzájem disjunktních kružnic.

V této sekci dokážeme následující větu:

Věta 8.3 (AC)**.** *$\mathbb{R}^3$ je sjednocením navzájem disjunktních jednotkových kružnic.*

Pro důkaz této věty se nám bude hodit znát *kardinální čísla*. Podobně jako ordinály reprezentují *typy* dobře uspořádaných množin, kardinály reprezentují *velikosti* dobře uspořádaných množin. Podrobněji se jim budeme věnovat v Sekci 9, ale zatím si je aspoň definujeme.

Definice 8.4 (Kardinální číslo)**.** Ordinál κ je *kardinální číslo*, pokud

$$(\forall \alpha \in \mathrm{On})(\alpha < \kappa \implies \alpha \prec \kappa).$$

Pokud množina x splňuje $x \approx \kappa$ pro nějaký kardinál κ, pak definujeme $|x| \coloneqq \kappa$ a říkáme, že κ je *mohutnost* (nebo *kardinalita*) množiny x. Snadno se ukáže že mohutnost $|x|$ je definovaná $\iff$ množinu x lze dobře uspořádat. Ovšem jelikož předpokládáme axiom výběru, tak *každou* množinu lze dobře uspořádat. Speciálně lze uspořádat množinu reálných čísel. Její mohutnost značíme

$$|\mathbb{R}| = \mathfrak{c}$$

a nazýváme ji *kontinuum.*

Dále se nám bude hodit následující fakt:

Fakt 8.5 (AC)**.** *Pokud jsou A a B nekonečné množiny, potom*

$$|A \cup B| = |A \times B| = \max\big\{|A|,|B|\big\}.$$

Navíc pokud $|A| > |B|$, pak $|A \setminus B| = |A|$.

Tedy speciálně $|A \times A| = |A|$ a indukcí $|A^n| = |A|$ pro každé nenulové $n \in \omega$.

Důkaz Věty 8.3. Podle předchozího faktu $|\mathbb{R}^3| = \mathfrak{c}$, tudíž můžeme $\mathbb{R}^3$ dobře uspořádat podle typu $\mathfrak{c}$ a očíslovat body $x \in \mathbb{R}^3$ ordinálními čísly jako

$$\mathbb{R}^3 = \{x_\alpha \,|\, \alpha < \mathfrak{c}\}.$$

Pomocí transfinitní rekurze nyní definujeme množinu $\big\langle C_\alpha \,|\, \alpha < \mathfrak{c} \big\rangle$ disjunktních (až na identické opakování, jak záhy zdůvodníme) jednotkových kružnic $C_\alpha \subseteq \mathbb{R}^3$ tak, aby vždy $x_\alpha \in C_\alpha$, a tudíž

$$\bigcup_{\alpha<\mathfrak{c}} C_\alpha = \mathbb{R}^3.$$

Všimněme si, že se může stát, že v době kdy se dostaneme k ordinálu α, jsme bod x_α již pokryli nějakou kružnicí C_β pro $\beta < \alpha$. Potom prostě položíme $C_\alpha \coloneqq C_\beta$. Tyto dvě kružnice sice nebudou disjunktní, ale to nevadí, protože jde o jednu a tu samou kružnici

Předpokládejme, že jsme v kroku $\alpha < \mathfrak{c}$, a body x_β pro $\beta < \alpha$ jsme již pokryli kružnicemi C_β pro $\beta < \alpha$. Pokud x_α leží na nějaké z kružnic C_β, položíme $C_\alpha \coloneqq C_\beta$. Jinak již zkonstruované kružnice C_β definují méně než $\mathfrak{c}$ zakázaných nadrovin (nejhorší případ: všechny kružnice leží v různých nadrovinách). Bodem x_α ovšem prochází celkem $|\mathbb{R} \times \mathbb{R}| = \mathfrak{c}$ nadrovin (každá nadrovina je určena třemi body). Tedy existuje nadrovina H procházející bodem x_α, ve které neleží žádná z kružnic C_β pro $\beta < \alpha$.

Může se stát, že některá z již zkonstruovaných kružnic C_β nadrovinu H protíná; buď v jednom, nebo ve dvou bodech. Průsečíků je ovšem méně než $\mathfrak{c}$:

$$P \coloneqq \bigcup_{\beta<\alpha} (H \cap C_\beta) \preceq 2 \times \alpha \approx \alpha \prec \mathfrak{c}.$$

Chceme najít nějakou kružnici co leží v nadrovině H, ale neprotíná žádný z průsečíků $p \in P$. Každý bod $p \in P$ určuje nejvýše 2 jednotkové kružnice procházejících body x_α a p. Počet zakázaných kružnic je tedy nejvýše $|2 \times P| < \mathfrak{c}$. Protože jednotkových kružnic $C \subseteq H$ procházejících bodem $x_\alpha \in H$ je kontinuum mnoho, tak pomocí axiomu výběru[13] lze zvolit kružnici $C_\alpha \subseteq H$ procházející bodem x_α, která není zakázaná. Tudíž $x_\alpha \in C_\alpha$, a navíc $C_\beta \cap C_\alpha = \varnothing$ pro každé $\beta < \alpha$.

Až transfinitní rekurze „magicky“ doběhne až k $\mathfrak{c}$, budeme mít hotovo. □

Úloha 8.6 (AC)**.** Dokažte, že v $\mathbb{R}^2$ existuje množina, která má s každou přímkou společné právě dva body. Hyperbola je k tomu docela blízko, ale ne úplně.

Nápověda. Použijte podobnou strategii jako v důkazu předchozí věty.

8.2 Kumulativní hierarchie množin

Motivace pro tuto sekci je následující: v teorii grafů často „ztotožňujeme“ izomorfní grafy, protože nás zajímá pouze jejich struktura, ne pojmenování vrcholů. Ale jak to udělat formálně?

Konečné grafy a grafy s omezenou velikostí Pokud pracujeme pouze s konečnými grafy, můžeme bez újmy na obecnosti předpokládat, že jejich vrcholy jsou přirozená čísla. V takovém případě existuje pouze spočetně mnoho neizomorfních grafů a každá třída izomorfismu je spočetná; formálně tak lze pracovat buď s třídami izomorfismu, nebo pomocí axiomu výběru zvolit z každé třídy nějakého kanonického reprezentanta. Podobná je i situace, kdy uvažujeme pouze grafy, jejichž velikost je omezena nějakým kardinálem κ.

Problém se třídou všech grafů Pokud však připustíme grafy libovolné nekonečné velikosti, pak oba tyto přístupy selžou. Neizomorfních grafů je vlastní třída (kardinálů je vlastní třída a pro každý kardinál κ můžeme definovat úplný graf na κ vrcholech), takže výběr reprezentanta z každé třídy izomorfismu by vyžadoval selektor na vlastní třídě, což nám axiom výběru neposkytuje. Navíc každá z tříd izomorfismu je rovněž vlastní třídou (a to i za předpokladu, že oborem vrcholů grafů jsou pouze ordinální čísla). Třída tříd izomorfismu tudíž neexistuje (vlastní třídy nemohou být prvky jiných tříd), a tak nemůžeme pracovat ani s třídami izomorfismu. Mohli bychom ještě více omezit, co považujeme za graf (co mohou být vrcholy), a možná by se nám povedlo zajistit, že třídy izomorfismu by byly množiny; existuje však mnohem elegantnější způsob známý jako *Scottův trik*.

[13] Formálně použijeme selektor na množině $\mathcal{P}\big(\{C \mid C \text{ je jednotková kružnice v } \mathbb{R}^3\}\big)$.

Scottův trik a typy grafů Každému grafu G přiřadíme množinu $\tau(G)$ zvanou jeho *typ*, takovou, že

$$G \cong H \iff \tau(G) = \tau(H).$$

Typ grafu nám tedy poskytuje veškeré informace spojené s jeho strukturou až na izomorfismus, což nám umožňuje formálně pracovat s typy grafů.

Kumulativní hierarchie množin Nepůjdeme do detailů, ale hlavní myšlenka je definovat hierarchii množin

$$V_0 \coloneqq \varnothing, \quad V_{\alpha+1} \coloneqq \mathcal{P}(V_\alpha), \quad V_\lambda \coloneqq \bigcup_{\alpha<\lambda} V_\alpha$$

kde λ je limitní ordinál. Z axiomu fundovanosti se pak dá dokázat (dokonce mu to je ekvivalentní), že každá množina x se dříve nebo později objeví v nějakém kroku V_α. Díky tomu lze definovat *rank* množiny x jako

$$\varrho(x) \coloneqq \min\{\alpha \mid x \subseteq V_\alpha\}.$$

Typ grafu G pak definujeme jako množinu

$$\tau(G) \coloneqq \Big\{H \;\Big|\; H \cong G \wedge (\forall H')\big(H' \cong G \Rightarrow \varrho(H) \leq \varrho(H')\big)\Big\}.$$

Typ grafu G je tedy množina všech jemu izomorfních grafů s minimálním možným rankem α. Všimněme si, že to opravdu je množina, protože $\tau(G) \subseteq V_{\alpha+1}$.

Úloha 8.7. Nechť $(A, \leq)$ je částečně uspořádaná vlastní třída s tou vlastností, že každá neprázdná podmnožina $B \subseteq A$ obsahuje minimální prvek. Dokažte, že potom dokonce každá neprázdná *podtřída* $B \subseteq A$ obsahuje minimální prvek.

Poznámka. To, že zde kvantifikujeme vlastní třídy, je v pořádku, viz konec Sekce 4.1.

Nápověda. Pro spor předpokládejte, že nějaká podtřída $B \subseteq A$ neobsahuje žádný minimální prvek, a pokuste se najít podmnožinu $X \subseteq B$, která také nemá žádný minimální prvek. Využijte, že každá úroveň V_α kumulativní hierarchie je množinou.

9 Kardinální čísla

V této sekci poskytneme ochutnávku navazujícího předmětu NMAI074. Všechny důkazy a podrobnější vysvětlení lze najít ve skriptíčkách [6] k tomuto předmětu.

Podobně jako ordinální čísla reprezentují typy uspořádání dobře uspořádaných množin, *kardinální čísla* reprezentují *velikosti* dobře uspořádaných množin.

Definice 9.1 (Kardinální číslo)**.** Ordinál κ je *kardinální číslo*, pokud

$$(\forall \alpha \in \mathrm{On})(\alpha < \kappa \implies \alpha \prec \kappa).$$

Třídu všech kardinálních čísel označíme Cn.

Každé $n \in \omega$ a ω jsou kardinální čísla. Pokud $\alpha \geq \omega$, pak $\alpha + 1$ není kardinální číslo; tudíž každé nekonečné kardinální číslo je limitní ordinální číslo. Ne každé limitní ordinální číslo je ale kardinální číslo: například $\omega + \omega > \omega$, ale $\omega + \omega \approx \omega$, takže $\omega + \omega$ není kardinální číslo. Podle stejné úvahy není žádný spočetný ordinál $\alpha > \omega$ kardinální číslo. Na druhou stranu, první nespočetný ordinál ω_1 je kardinální číslo.

Pokud množina x splňuje $x \approx \kappa$ pro nějaký kardinál κ, pak definujeme $|x| := \kappa$ a říkáme, že κ je *mohutnost* (nebo *kardinalita*) množiny x. Všimněme si, že pokud je α ordinál, pak $|\alpha| \leq \alpha$, a navíc jsou následující tvrzení ekvivalentní:

(1) $|\alpha| = \alpha$,

(2) α je kardinální číslo,

(3) α je první ordinál s mohutností $|\alpha|$.

Pozorování 9.2. *Pokud mají množiny x a y definované své mohutnosti, pak*

(a) $x \approx y \iff |x| = |y|$,

(b) $x \approx |x|$.

Pozorování 9.3. *Mohutnost $|x|$ je definována $\iff$ x lze dobře uspořádat.*

Důkaz. Pokud lze x dobře uspořádat, pak $|x|$ je nejmenší typ uspořádání z dobrých uspořádání množiny x, jelikož každé z těchto uspořádání indukuje bijekci mezi x a ordinálním typem daného uspořádání. Na druhou stranu, pokud je $|x| = \kappa$ definováno, pak můžeme x dobře uspořádat přenesením uspořádání z κ. □

9.1 Alefy

Kardinální čísla jsou uzavřená na suprema: Pokud by $\lambda = \sup \kappa_i$ nebyl kardinál, pak $|\lambda| < \lambda$. Protože je λ supremum, existuje nějaké κ_j takové, že $|\lambda| < \kappa_j \leq \lambda$. To je ale ve sporu s tím, že κ_j je kardinál.

Lze také ukázat, že pro každý kardinál existuje větší kardinál. Proto je třída všech kardinálů Cn vlastní třída; jinak by její supremum bylo největším kardinálem. Z toho, že Cn je vlastní třída ordinálů uzavřená na suprema, lze dokázat, že existuje jednoznačně určené, rostoucí, bijektivní zobrazení $\aleph\colon \mathrm{On} \to \mathrm{Cn} \setminus \omega$, enumerující nekonečná kardinální čísla, které splňuje $\aleph(\alpha) = \sup\{\aleph(\beta) \mid \beta < \alpha\}$ pro každý limitní ordinál α. Cantor zavedl pro označení této funkce symbol $\aleph$ („alef"), první písmeno hebrejské abecedy; její hodnoty $\aleph(\alpha)$ se značí jako $\aleph_\alpha$.

Historicky nebyly ordinály a kardinály konkrétní množiny, ale abstraktní koncepty: ordinály popisovaly typy dobrého uspořádání, zatímco kardinály měřily velikost. Toto rozlišení vedlo k vývoji dvou paralelních systémů značení, ω_α a $\aleph_\alpha$. Von Neumannova množinová definice ordinálů tyto myšlenky sjednotila tím, že poskytla kanonické reprezentanty pro typy dobrých uspořádání. Dnes často píšeme ω_α, když uvažujeme kardinál $\aleph_\alpha$ jakožto ordinál s jeho dobrým uspořádáním. Konkrétně první nespočetný ordinál se značí jako ω_1, a první nekonečný kardinál jako $\aleph_0 = \omega$.

Následník kardinálu κ je nejmenší kardinál větší než κ a značíme ho κ^+. Dále říkáme, že κ je *předchůdce* kardinálu κ^+. Pokud kardinál λ nemá žádného předchůdce a $\lambda \neq 0$, tak je *limitní*; jinak je *izolovaný*.

Příklad. Zjevně $\aleph_{\alpha+1} = \aleph_\alpha^+$ jsou izolované kardinály a $\aleph_0$ je limitní kardinál. Je snadné ukázat, že $\aleph_\alpha$ pro $\alpha > 0$ je limitní kardinál $\iff$ α je limitní ordinál.

9.2 Vlastnosti nekonečných kardinálů

Definice 9.4. Pokud jsou κ a λ kardinální čísla, definujeme kardinály

(a) $\kappa + \lambda \coloneqq |(\{0\} \times \kappa) \cup (\{1\} \times \lambda)|$,

(b) $\kappa \cdot \lambda \coloneqq |\lambda \times \kappa|$,

Jinými slovy, $\kappa + \lambda$ a $\kappa \cdot \lambda$ jsou kardinální čísla, která reprezentují velikost množiny na pravé straně rovnice, zatímco ordinální sčítání a násobení vyjadřují typ uspořádání téže množiny při lexikografickém uspořádání. Všimněme si, že kardinální sčítání a násobení jsou asociativní, komutativní a distributivní. Ordinální sčítání a násobení jsou asociativní, ale obecně nejsou komutativní ani distributivní zprava. Intuitivně je to proto, že ordinální operace si musí pamatovat uspořádání daných ordinálů.

Věta 9.5. *Pro každý ordinál α platí $|\aleph_\alpha \times \aleph_\alpha| = \aleph_\alpha$.*

Z toho není těžké ukázat, že pokud jsou κ a λ kardinály a alespoň jeden z nich je nekonečný, pak $\kappa + \lambda = \max\{\kappa, \lambda\}$. Pokud jsou navíc nenulové, pak $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$. Při aplikaci na nekonečné množiny dostáváme:

Důsledek 9.6 (AC)**.** *Pokud jsou A a B nekonečné množiny, potom*

$$|A \cup B| = |A \times B| = \max\big\{|A|,|B|\big\}.$$

Dále, pokud $|A| > |B|$, pak $|A \setminus B| = |A|$.

Lemma 9.7 (AC)**.** *Pro libovolnou množinu S platí, že $|\bigcup S| \leq |S| \cdot \sup\{|A| \mid A \in S\}$.*

Důsledek 9.8 (AC)**.** *Sjednocení libovolného systému $\aleph_\alpha$ množin, z nichž každá má mohutnost nejvýše $\aleph_\alpha$, má mohutnost nejvýše $\aleph_\alpha$.*

9.3 Regulární kardinály

Dirichletův princip říká, že ω nelze rozdělit na konečně mnoho konečných množin, neboli ekvivalentně, že pokud je $A \subseteq \omega$ konečná, pak $\sup(A) < \omega$. Kardinál $\aleph_0 = \omega$ tedy není možné „dosáhnout“ zespodu pomocí žádné podmnožiny s menší mohutností. Nekonečné kardinály s touto vlastností se nazývají *regulární*.

Definice 9.9 (Kofinalita)**.** Podmnožina $A \subseteq \alpha$ limitního ordinálu α je *kofinální* v α, pokud $\sup(A) = \alpha$ (limitou rostoucí posloupnosti prvků A je α). *Kofinalita* α je „délka“ nejkratší rostoucí posloupnosti s limitou α:

$$\operatorname{cf}(\alpha) \coloneqq \min\big\{ \text{typ uspořádání } (A, \leq) \,\big|\, A \subseteq \alpha \wedge \sup(A) = \alpha \big\}.$$

Lze ukázat, že $\mathrm{cf}(\alpha)$ je rovna minimální velikosti $|A|$ kofinální podmnožiny $A \subseteq \alpha$, takže kofinalita je vždy nekonečný kardinál. Proto $\omega \leq \mathrm{cf}(\alpha) \leq |\alpha|$.

Definice 9.10 (Regulární kardinál)**.** Nekonečné kardinální číslo κ je *regulární kardinál*, pokud $\mathrm{cf}(\kappa) = \kappa$, a *singulární kardinál* v opačném případě.

Regulární kardinály se chovají podobně jako ω v tom, že jsou *téměř* uzavřené na suprema: dokud je délka posloupnosti menší než κ, limita nikdy nedosáhne κ. Ekvivalentně to můžeme vyjádřit pomocí sjednocení menších množin.

Věta 9.11. *Nekonečné kardinální číslo κ je singulární $\iff$ existuje množina X taková, že $\kappa = \bigcup X$, kde $|X| < \kappa$ a $|x| < \kappa$ pro všechna $x \in X$.*

Důsledek 9.12 (AC)**.** *Každý nekonečný izolovaný kardinál $\aleph_{\alpha+1}$ je regulární.*

Důkaz. Kdyby byl singulární, podle předchozí věty by se dal zapsat jako sjednocení nejvýše $\aleph_\alpha$ množin mohutnosti nejvýše $\aleph_\alpha$. Ale potom by podle Důsledku 9.8 sám měl mohutnost nejvýše $\aleph_\alpha$, což je spor. □

9.4 Kardinální aritmetika

Kardinální aritmetika studuje nekonečné součty a součiny kardinálních čísel, a také vlastnosti kardinální mocniny. My se zaměříme pouze na kardinální mocninu.

Definice 9.13. Pro kardinální čísla κ a λ definujeme kardinál

$$\kappa^\lambda := |{}^\lambda\kappa| = |\{f \mid f \colon \lambda \to \kappa\}|.$$

Poznámka. Aby definice kardinální mocniny κ^λ dávala dobrý smysl, tak musíme předpokládat axiom výběru. Jinak by množinu na právě straně rovnice nemuselo jít dobře uspořádat a její mohutnost by nebyla definovaná. Proto budeme ve zbytku této sekce vždy předpokládat axiom výběru.

Všimněme si, že $2^\lambda = |\mathcal{P}(\lambda)|$, jelikož $\mathcal{P}(\lambda) \approx {}^\lambda 2$. Speciálně $|\mathbb{R}| = 2^\omega$. Cantorova věta tedy říká, že pro každý kardinál κ platí $\kappa < 2^\kappa$.

Pozorování 9.14. *Pro libovolné kardinály κ, λ a $n \in \omega$ platí*

(a) $0^0 = 1, \qquad \lambda > 0 \implies 0^\lambda = 0,$

(b) $\kappa^0 = 1, \qquad 1^\lambda = 1,$

(c) *pokud $\kappa \geq \omega$ a $n > 0$, pak $\kappa^n = \kappa$.* *. . . indukcí z $\kappa \cdot \kappa = \kappa$*

Úloha 9.15. Dokažte z definice kardinální mocniny, že platí

(a) pokud $0 < \kappa \leq \mu$ a $\lambda \leq \nu$ potom $\kappa^\lambda \leq \mu^\nu$,

(b) $\kappa^{\mu+\nu} = \kappa^\mu \cdot \kappa^\nu$,

(c) $(\kappa^\mu)^\nu = \kappa^{\mu\cdot\nu}$.

Tudíž pro kardinální mocninu platí klasická pravidla pro práci s exponenty.

Věta 9.16. *Pro libovolné kardinály κ a $\lambda \geq \aleph_0$ platí, že*

(a) *pokud $2 \leq \kappa \leq \lambda$, potom $\kappa^\lambda = 2^\lambda$,* *. . . speciálně $\kappa^\kappa = 2^\kappa$*

(b) *pokud $\lambda \leq \kappa$, potom $(\kappa^+)^\lambda = \kappa^\lambda \cdot \kappa^+$,* *. . . speciálně $(\kappa^+)^\kappa = 2^\kappa \cdot \kappa^+ = 2^\kappa$*

(c) *pokud κ je limitní kardinál a $\lambda < \mathrm{cf}(\kappa)$, potom $\kappa^\lambda = \sup_{\mu<\kappa} \mu^\lambda$,*

(d) *pokud $\lambda \geq \mathrm{cf}(\kappa)$, potom $\kappa^\lambda > \kappa$.*

9.5 Zobecněná hypotéza kontinua

Připomeňme, že hypotéza kontinua (CH) tvrdí, že neexistuje žádná množina x taková, že $\omega \prec x \prec \mathbb{R}$. Pomocí kardinální mocniny ji můžeme v ZFC zapsat jako

$$2^{\aleph_0} = \aleph_1.$$

Zobecněná hypotéza kontinua (GCH) tvrdí, že

$$(\forall \alpha \in \mathrm{On}) : 2^{\aleph_\alpha} = \aleph_{\alpha+1}.$$

Gödel (1940) dokázal, že GCH je konzistentní s ZFC, a Cohen (1963) dokázal, že její negace $\neg$GCH je také konzistentní.

Čili to, zda zobecněné hypotéze kontinua věříme, je čistě filozofické rozhodnutí; z pohledu logiky jsou obě možnosti stejně dobré. Ovšem z pohledu kardinální aritmetiky je platnost GCH určitě výhodnější, protože trivializuje výpočet kardinálních mocnin:

Úloha 9.17. Dokažte, že z GCH plyne, že pro libovolné kardinály $\kappa \geq \aleph_0$ a λ platí

(i) pokud $0 < \lambda < \mathrm{cf}(\kappa)$, pak $\kappa^\lambda = \kappa$,

(ii) pokud $\mathrm{cf}(\kappa) \leq \lambda \leq \kappa$, pak $\kappa^\lambda = \kappa^+$,

(iii) pokud $\kappa \leq \lambda$, pak $\kappa^\lambda = \lambda^+$.

Nápověda. Použijte Větu 9.16 a transfinitní indukci podle α, kde $\kappa = \aleph_\alpha$.

9.6 Velké kardinály

Víme, že $\aleph_0$ je regulární a že v ZFC je každý nekonečný izolovaný kardinál $\aleph_{\alpha+1}$ také regulární. Možná poněkud překvapivě nelze z axiomů ZFC dokázat existenci jiného limitního regulárního kardinálu než $\aleph_0 = \omega$, protože by to umožnilo zkonstruovat model ZFC uvnitř ZFC, což by bylo ve sporu s Gödelovou druhou větou o neúplnosti (ZFC by dokázala svoji vlastní konzistenci). Tyto hypotetické kardinály poprvé navrhl Felix Hausdorff v roce 1908, a dnes je nazýváme *slabě nedosažitelné*. Pokud slabě nedosažitelný kardinál κ navíc splňuje, že pro všechny kardinály $\lambda < \kappa$ platí $2^\lambda = |\mathcal{P}(\lambda)| < \kappa$, pak je κ *silně nedosažitelný.*[14]

Mnoho problémů v teorii množin a nekonečné kombinatorice vede na otázku, zda existují kardinály s určitými vlastnostmi. Pokud existenci takových kardinálů nelze v ZFC dokázat, nazývají se *velké kardinály.* Tvrzení, která prohlašují, že takové kardinály existují, se občas nazývají *silné axiomy nekonečna* a tvoří neuvěřitelné komplexní hierarchii. Nedosažitelné kardinály jsou ty nejslabší z těchto axiomů.

Některá tvrzení lze dokázat pouze za předpokladu příslušných velkých kardinálů. Potom je potřeba mít víru v korektnost takového předpokladu, protože ZFC nemůže dokázat jeho bezespornost.

Slabě kompaktní kardinály Uvedeme ještě jeden druh velkých kardinálů. Slavná Ramseyova věta říká, že pokud obarvíme hrany úplného grafu na $\aleph_0 = \omega$ vrcholech červeně a modře, tak vždy najdeme nekonečnou jednobarevnou kliku.

Ovšem ZFC neumí dokázat existenci žádného dalšího kardinálu s touto vlastností: nespočetného kardinálu κ, který splňuje, že kdykoli obarvíme hrany úplného grafu na κ vrcholech červeně a modře, tak vždy najdeme jednobarevnou kliku velikosti κ. Kardinální čísla s touto vlastností se nazývají *slabě kompaktní*, a jelikož se dá dokázat, že musí být silně nedosažitelná, tak jsou to velké kardinály.

[14] Důvod, proč existenci silně nedosažitelného kardinálu κ není možné dokázat, je ten, že by úroveň V_κ kumulativní hierarchie množin (viz Sekce 8.2) už byla dost uzavřená na to, aby splňovala všechny axiomy ZFC. Jinými slovy bychom byli schopni zevnitř ZFC dokázat, že ZFC má model.

Zdroje

[1] Bohuslav Balcar a Petr Štěpánek. *Teorie množin*. Vydání 2., opravené a rozšířené. Praha: Academia, 2001.

[2] Stack Exchange. *Examples of bijective map from* $\mathbb{R}^3 \to \mathbb{R}$. Navštíveno 26. června 2026. URL: `https://math.stackexchange.com/q/183361`.

[3] Gina Garcia Tarrach. „The Axiom of Choice and its implications in mathematics". Dipl. pr. Universitat de Barcelona, 2017. URL: `https://hdl.handle.net/2445/121981`.

[4] Gro-Tsen a IkamusumeFan. *Visual representation of the ordinal* ω^2. `https://commons.wikimedia.org/wiki/File:Ordinal_ww.svg` (accessed 11 March 2026). 2015.

[5] Mirek Olšák. *Matematický korespondenční seminář: Do nekonečna a ještě dál.* Navštíveno 20. prosince 2023. URL: `https://prase.cz/archive/35/serial.pdf`.

[6] Jakub Smolík. *Infinite Sets*. Navštíveno 15. května 2026. URL: `https://couleslaw.github.io/infinite-sets.pdf`.